



AKER Report Center



AKER

www.aker.com.br



Índice

Índice	2
Índice de Figuras.....	5
1 Aker Report Center	12
1.1 Como está disposto este manual.	12
1.2 Apresentação do Produto.....	12
2 Instalação	15
2.1 Instalação.....	15
2.2 Expandindo espaço em disco - LVM	28
2.3 Licenciamento.....	32
3 Dashboard	39
3.1 Aba Dashboard	39
3.2 Aba Relatórios Externos	42
3.3 Aba Aker Monitoring	44
3.4 Aba Pesquisa.....	45
4 Relatórios	48
4.1 Gerar Relatório	48
4.2 Fila de Relatórios	49
Relatórios gerados	50
4.3 Agendamento	51
Janela de agendamento de relatórios:	52
5 Cadastro	54
5.1 Entidades	54
5.2 Ativos	55
Cadastro de Ativos 	55
Cadastrando um novo Ativo	56
Aba Cadastro de ativo	57



Envio FTP	58
Envio Syslog.....	58
Aba Eventos Processados	60
Aba Eventos Não Processados.....	61
5.3 Colunas	62
5.4 Tipos de ativo.....	62
5.4.1 Adicionando um novo tipo de ativo:.....	63
5.5 Relatório	66
5.6 Relatórios personalizados.....	66
Criando um novo de relatório do tipo detalhado.....	66
Criando um novo de relatório do tipo Consolidado.....	70
5.7 Grupos de relatórios.....	74
6 Configurações.....	76
6.1 Autenticação.....	76
Perfis	77
Usuários	78
Usuários FTP	78
Tipo de autenticação	79
FTP TLS.....	80
6.2 Rede.....	80
Interface de rede	81
Servidores NTP	82
6.3 Backup	82
Realizar backup.....	83
Restaurar backup	83
6.4 Rotate	85
6.5 E-mail.....	86
6.6 Serviços.....	87
6.7 Exportação.....	89
6.8 Logs do sistema	90



6.9 Ajuda.....	91
6.10 <i>Licenciamento</i>	91
Gerar Chave	92
Atualizações	95
Fórum Aker.....	96
Manual.....	96
6.11 Opções de gerenciamento da conta do usuário	97



Índice de Figuras

Figura 1 - boot menu.....	16
Figura 2 - seleção de idioma	17
Figura 3 - Localidade	17
Figura 4 - configuração do teclado.....	18
Figura 5 - Carregando componentes adicionais	18
Figura 6 - Configurar a rede "nome da máquina"	19
Figura 7 - Configurar a rede "nome do domínio"	19
Figura 8 - Configurar usuários e senha	20
Figura 9 - confirmação de senha	20
Figura 10 - Nome completo para o novo usuário	21
Figura 11 - Nome de usuário para sua conta	21
Figura 12 - senha para novo usuário.....	21
Figura 13 - confirmação de senha	22
Figura 14 - configuração do relógio	22
Figura 15 - Particionar discos	23
Figura 16 - seleção de disco a ser particionado	23
Figura 17 - Esquema de particionamento	24
Figura 18 - Finalizar o particionamento e escrever as mudanças no disco	24
Figura 19 - Confirmação e mudanças.....	25
Figura 20 - instalando o sistema	25
Figura 21 - configurar o gerenciador de pacotes	25
Figura 22 - configurando o apt.....	26
Figura 23 - instalar o carregador de inicialização GRUB	26
Figura 24 - seleção de dispositivo para instalação do carregador de inicialização	26
Figura 25 - Instalando o carregador de inicialização GRUB	27



Figura 26 - Finalizar a instalação	27
Figura 27 - Visualizando IP para acesso no browser	27
Figura 28 - Acesso web.....	28
Figura 29 - Expandir a capacidade do disco	28
Figura 30 - comando fdisk -l /dev/sda	29
Figura 31 - digite 'N' para inserir uma nova partição	29
Figura 32 - digite 'p' para adicionar uma partição primária	30
Figura 33 - definindo o número da partição	30
Figura 34 - definindo o valor para o primeiro setor.....	30
Figura 35 - Informação dos setores	30
Figura 36 - Visualizando a nova partição	30
Figura 37 - mensagem de Warning	31
Figura 38 – Reiniciando a máquina para aplicar as mudanças	31
Figura 39 - comando para cria uma nova partição no LVM.....	31
Figura 40 - comando para expandir o volume do Aker Report Center.....	31
Figura 41 – comando utilizado para expandir o volume lógico da LVM.....	32
Figura 42 - comando para redimensionar o sistema de arquivos	32
Figura 43 - reiniciar o sistema para aplicar as alterações	32
Figura 44 - Mensagem ao errar a senha mais de 3 vezes	33
Figura 45 - Tela de login	33
Figura 46 - Gerar chave	34
Figura 47 - Localizando licença	35
Figura 48 - Opções de carregamento da licença.....	35
Figura 49 - Informação da licença	36
Figura 50 - Menus	37
Figura 51 - Abas do Dashboard	39
Figura 52 - Aba Dashboard.....	40



Figura 53 – Widget “Uso de CPU e Memória” atualizado em tempo real.....	40
Figura 54 – Widget “Total de eventos”	41
Figura 55 - Opções de período.....	41
Figura 56 - Widget "espaço utilizado em disco"	41
Figura 57 - Opções de Widget	41
Figura 58 - Relatórios Recebidos.....	42
Figura 59 - Ativos FTP.....	43
Figura 60 - Visualização de arquivos	44
Figura 61 - Aker Monitoring	45
Figura 62 - Aba Pesquisa	45
Figura 63 - Resultado da pesquisa	46
Figura 64 - Opções do menu Relatórios.....	48
Figura 65 - gerar relatório	48
Figura 66 - Fila de relatórios.....	49
Figura 67 - Relatórios gerados	50
Figura 68 - Relatórios gerados	51
Figura 69 - Agendamento de relatório.....	51
Figura 70 - janela de agendamento de relatórios.....	52
Figura 71 - menu cadastro	54
Figura 72 - Entidades.....	54
Figura 73 - Cadastro de entidades	55
Figura 74 - Cadastro de ativos.....	55
Figura 75 - Cadastro de ativos.....	56
Figura 76 - Aba Cadastro de ativo	56
Figura 77 - Configuração de envio via FTP	58
Figura 78 - Envio Syslog.....	58
Figura 79 - Parâmetros de configuração	59



Figura 80 - Aba log.....	60
Figura 81 - Aba Eventos processados.....	61
Figura 82 - Aba Eventos não processados.....	61
Figura 83 - cadastro de colunas	62
Figura 84 - Tipos de ativos	62
Figura 85 - Adicionando um novo tipo de ativo.....	63
Figura 86 - Adicionando um novo tipo de log.....	64
Figura 87 - Seleção de campos.....	65
Figura 88 - Campo de expressões regulares	65
Figura 89 - Menu relatório	66
Figura 90 - relatório.....	66
Figura 91 - Aba Relatório.....	67
Figura 92 - Aba Fonte de dados	68
Figura 93 - Aba Colunas.....	69
Figura 94 - Aba Parâmetros de filtro.....	70
Figura 95 - Opções de parâmetros de pesquisa.....	70
Figura 96 - Operador	70
Figura 97 - Aba Relatório.....	71
Figura 98 - Aba Fonte de dados	72
Figura 99 - Aba Colunas.....	72
Figura 100 - Aba Parâmetros de filtro.....	73
Figura 101 - Opções de parâmetros de pesquisa.....	73
Figura 102 - Operador	74
Figura 103 – Janela de criação de Grupo de relatórios.....	74
Figura 104 - menu configurações.....	76
Figura 105 – Autenticação	76
Figura 106 - Perfil	77



Figura 107 - Janela Perfil	77
Figura 108 - Usuários.....	78
Figura 109 - Usuários FTP.....	78
Figura 110 - Cadastro de usuário FTP	79
Figura 111 - Autenticação	79
Figura 112 - Configuração de segurança FTP	80
Figura 113 - rede	81
Figura 114 - Interface de rede.....	81
Figura 115 - Servidores NTP	82
Figura 116 - Opções de backup	83
Figura 117 -Janela Realizar Backup	83
Figura 118 - Criação de backup	83
Figura 119 - localizando arquivo de backup	84
Figura 120 - Janela Restaurar Backup	84
Figura 121 - Rotate.....	85
Figura 122 - Configuração de E-mail	86
Figura 123 - Janela de configuração de serviços.....	88
Figura 124 - Esquema de exportação de dados	89
Figura 125 - Janela de exportação de eventos.....	90
Figura 126 - Logs do sistema	91
Figura 127 - Mensagem ao errar a senha mais de 3 vezes	92
Figura 128 - Tela de login	92
Figura 129 - Gerar chave	93
Figura 130 - Localizando licença	94
Figura 131 - Opções de carregamento da licença.....	94
Figura 132 - Informação da licença	95
Figura 133 - Atualizações	96



Figura 134 - Opções para baixar atualizações.....	96
---	----

Aker Report Center





1 Aker Report Center

Seja bem-vindo ao manual do usuário do Aker Report Center.

Nos próximos capítulos você aprenderá como configurar esta poderosa ferramenta de gerenciamento de logs e criação de relatórios. Esta introdução tem como objetivo descrever a organização deste manual e tentar tornar sua leitura o mais simples e agradável possível.

1.1 Como está disposto este manual.

Este manual está organizado em vários capítulos. Cada capítulo mostrará um aspecto da configuração do produto e todas as informações relevantes ao aspecto tratado.

Todos os capítulos começam com uma introdução teórica sobre o tema a ser tratado, seguido dos aspectos específicos de configuração do **Aker Report Center**. Com esta introdução teórica, alguns módulos possuem exemplos práticos do uso do serviço a ser configurado, em situações hipotéticas, porém próximas da realidade do usuário. Com isso buscamos tornar o entendimento das diversas variáveis de configuração o mais simples possível.

Recomendamos que este manual seja lido pelo menos uma vez por inteiro, na ordem apresentada. Posteriormente, se necessário, use-o como fonte de referência (para facilitar seu uso como referência, os capítulos estão divididos em tópicos, com acesso imediato pelo índice principal. Desta forma, pode-se acessar facilmente a informação desejada).

Em vários locais deste manual, aparecerá o símbolo  seguido de uma frase escrita em **letras vermelhas**. Isto significa que a frase em questão é uma observação muito importante e deve ser totalmente entendida antes de prosseguir com a leitura do capítulo.

1.2 Apresentação do Produto

Se sua rede fosse vítima de um acesso não autorizado, como você iria detectar? Como você reagiria a tal ataque antes que fosse tarde para a proteção e integridade das informações de sua empresa? Você seria capaz de rastrear a origem do ataque? E se este ataque fosse de um usuário com acesso privilegiado, tentando causar algum dano à sua rede, como você descobriria?

Apesar da grande quantidade de dados armazenados nas máquinas das redes terem informações que são de extrema importância para a proteção e o gerenciamento de sua rede, a maioria das empresas não possuem os recursos necessários para, utilizar estes dados para



analisar todas estas informações efetivamente e em tempo real proporcionando maior segurança aos dados de sua empresa.

Visando oferecer maior proteção à segurança da informação de seus clientes a **Aker Security Solutions** desenvolveu o **Aker Report Center**.

Uma poderosa ferramenta que oferece a você e sua rede, gerenciamento de logs, análise preditiva capaz de descobrir padrões suspeitos nos dados coletados, os quais olhos humanos não conseguem detectar, geração de relatórios em diversos modelos de acordo com a necessidade de sua empresa nos formatos **HTML**, **TXT** e **PDF**, visualização de relatórios e gráficos personalizados, filtragem de logs customizada, agendamento de geração de relatórios, acesso seguro e flexibilidade ao receber dados não apenas dos produtos da Aker Security Solutions (**Aker Firewall 6.5, 6.7 e 6.8**), mas também das principais soluções de segurança da informação disponíveis no mercado.

Características

- Suporta mais de 370 tipos de ativos;
- Relatórios em HTML, PDF e TXT;
- Integração com ativos de terceiros;
- Dashboard personalizável e responsivo.

Vantagens

- Alta performance;
- Ambiente escalável e flexível;
- Interface Web de fácil configuração e em português;
- Gerenciamento de logs via dispositivo móvel;
- Simplificação da gestão da infraestrutura de TI.

Instalação





2 Instalação

Neste capítulo será abordado o procedimento de instalação e licenciamento do Aker Report Center.

Para que o **Aker Report Center** execute de maneira satisfatória, recomenda-se que as configurações descritas a seguir sejam atendidas:

Aker Report Center IS/VM

- 8 GB memória RAM;
- 160 GB de espaço em disco disponível;



Para máquinas que possuem 16 GB de memória ou mais, é recomendado que seja direcionado apenas metade da memória para o cache. Exemplo: A máquina do usuário possui 32 GB de memória, desta forma deve-se editar o arquivo “/etc/mongod.conf” definindo a metade (16 GB) da memória para o cache. Arquivo: /etc/mongod.conf
Linha: cacheSizeGB: 16

O Aker Report Center sobre o sistema operacional Debian 64 bits.

2.1 Instalação

O Aker Report Center pode ser adquirido na forma de software (IS/VM).

A seguir os procedimentos para instalar o Aker Report Center.

- Efetue o download da imagem do Aker Report Center para IS/VM na página de download no site da Aker: <http://www.aker.com.br/produtos/aker-report-center/downloads/>
- Em seguida, abra a imagem do Aker Report Center no virtualizador desejado e inicia a máquina.
- Na tela inicial do instalador do Aker Report Center selecione a opção “Instalar o Aker Report Center” e pressionar a tecla “Enter”.

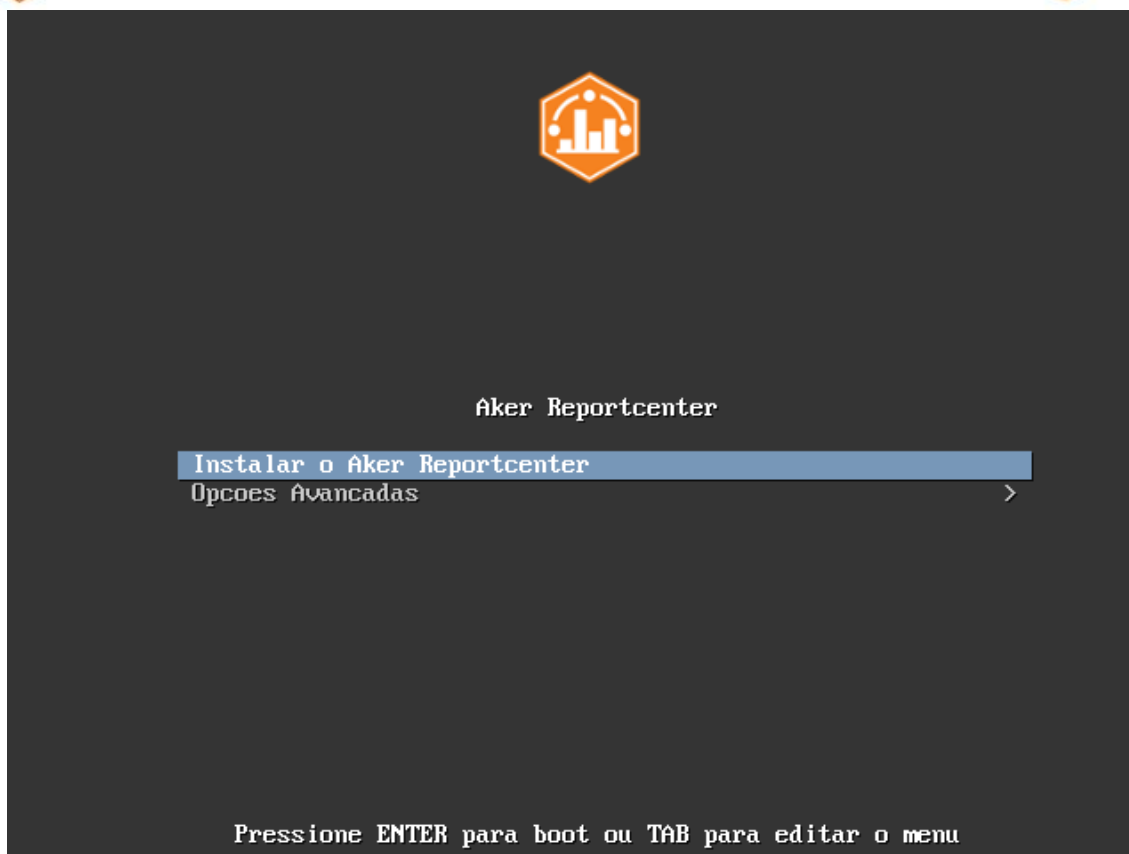


Figura 1 - boot menu

- Nesta exibida a seguir, o usuário deve selecionar o idioma que a instalação será executada. Ao selecionar o idioma desejado, pressione a tecla “**Enter**”.

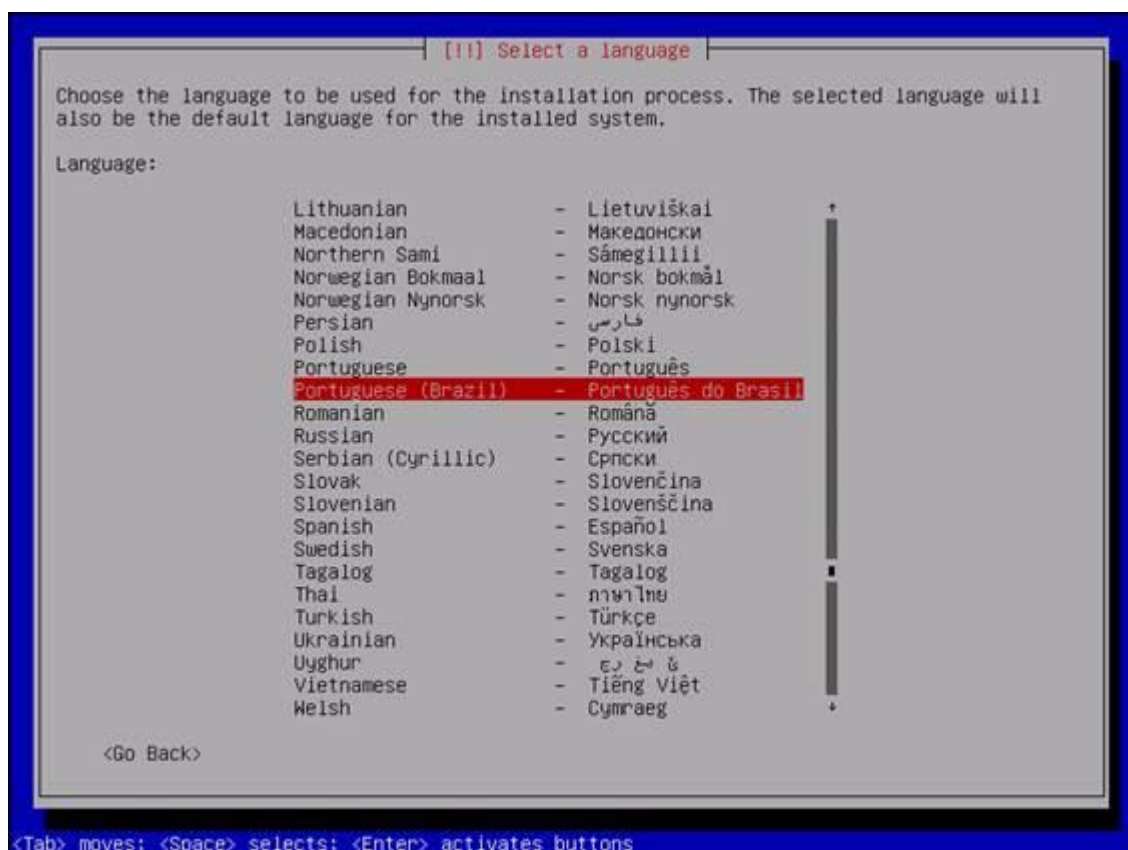




Figura 2 - seleção de idioma

- Ao selecionar o idioma Português, será necessário informar a localização (*País, Território ou Área*). Selecione a opção desejada e pressione a tecla “Enter”.

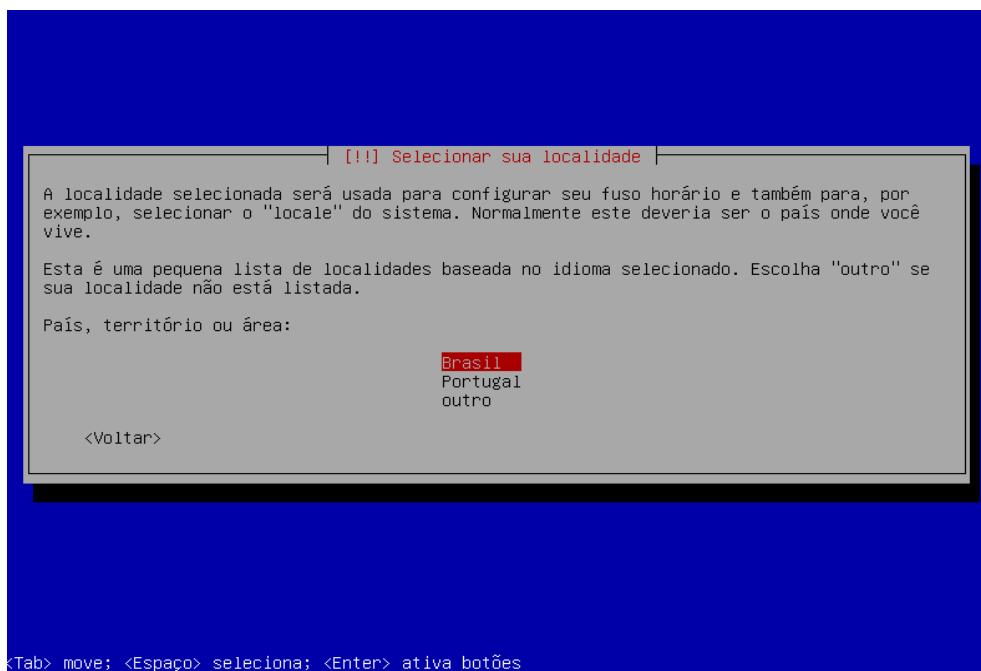


Figura 3 - Localidade

- Em seguida, selecione o idioma de configuração do teclado. Ao selecionar o idioma desejado e pressione a tecla “Enter”.

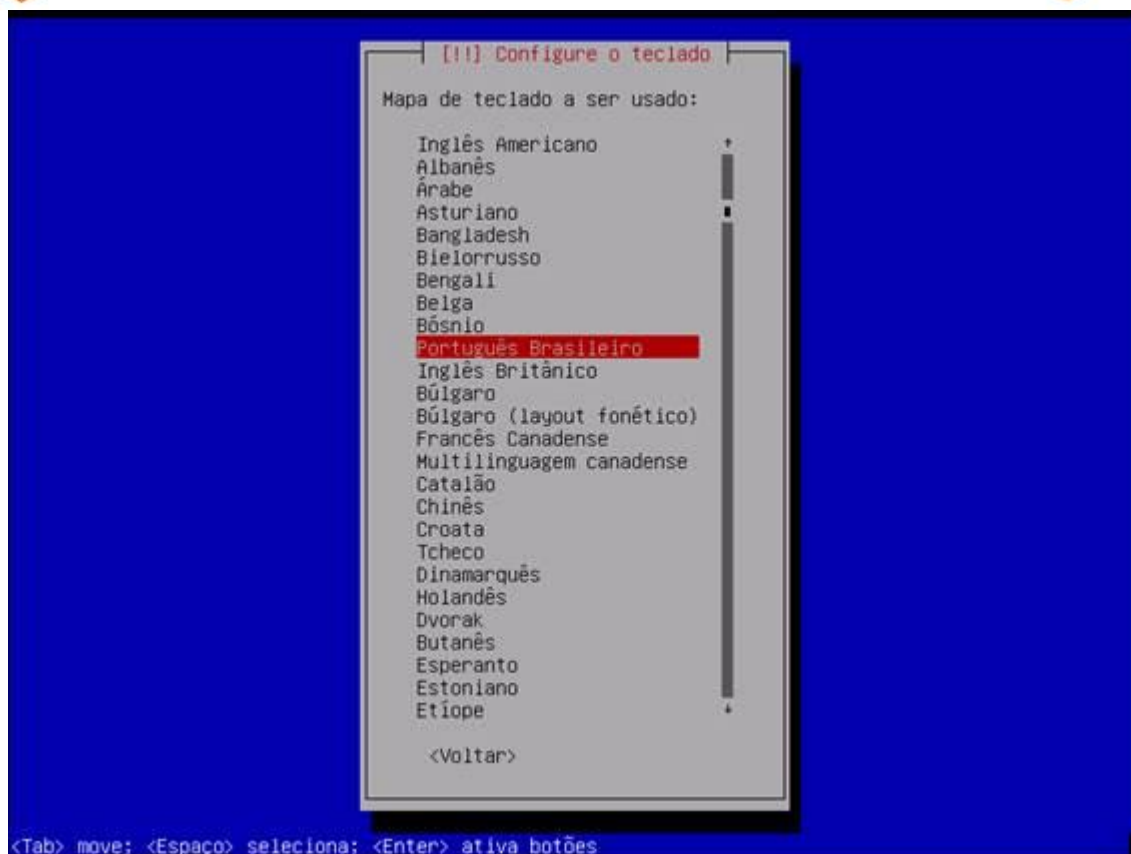


Figura 4 - configuração do teclado

- Aguarde o carregamento dos componentes adicionais e prossiga para a configuração da rede.

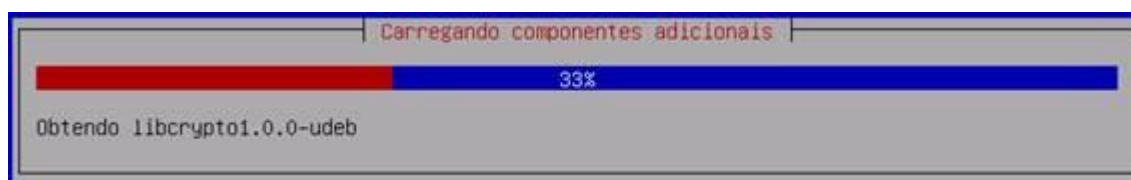


Figura 5 - Carregando componentes adicionais

- Na tela de configuração de rede o usuário deve definir o nome da máquina (hostname). Defina o nome desejado e pressione a tecla “**Enter**”.

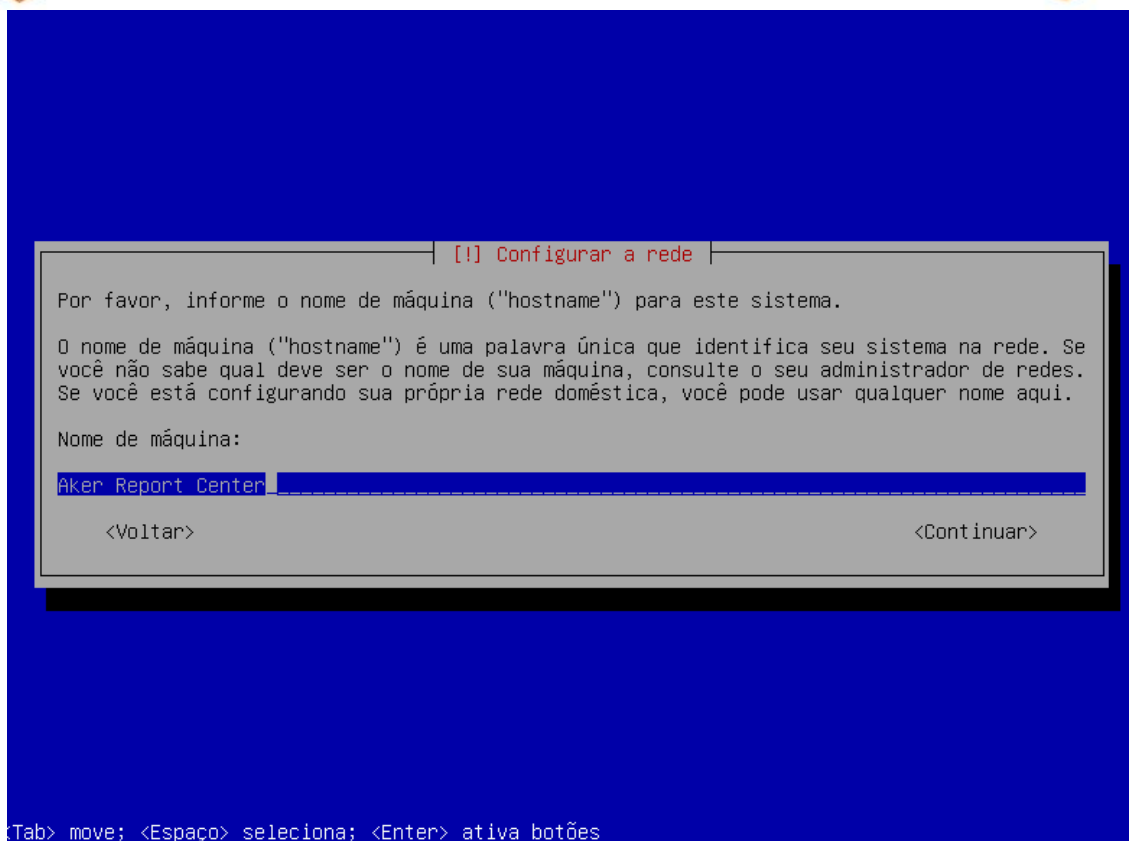


Figura 6 - Configurar a rede "nome da máquina"

- Na janela a seguir, o usuário deve informar o nome do domínio de sua rede. Caso não possua um domínio, simplesmente deixe este campo em branco, e pressione a tecla **"Enter"** para continuar.

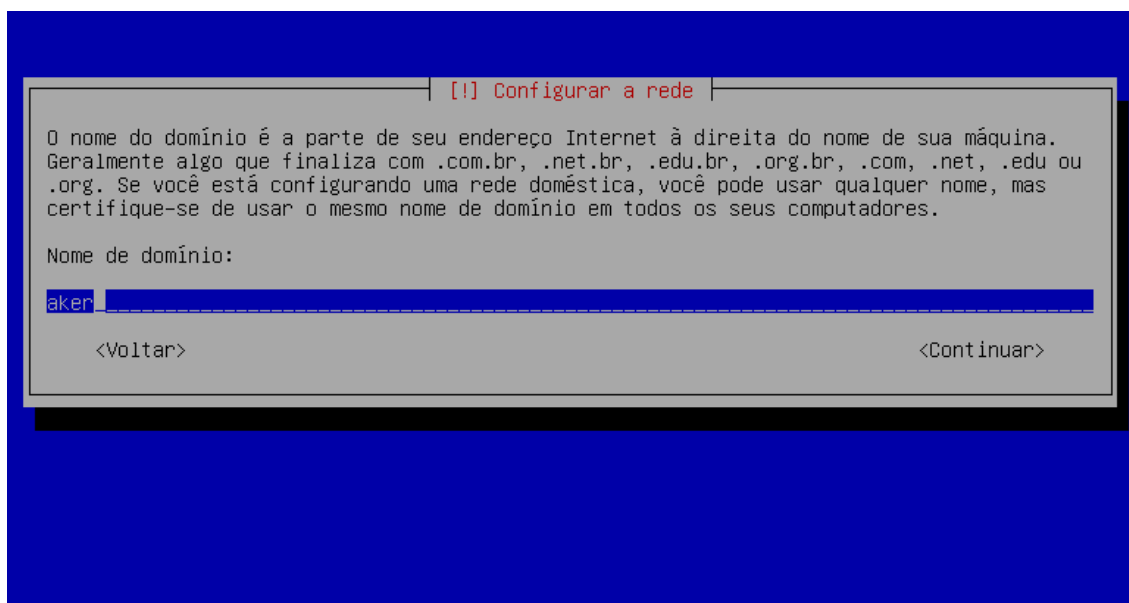


Figura 7 - Configurar a rede "nome do domínio"



- Em seguida, o usuário deve definir a senha de Root do Sistema. Ao definir a senha de “root” pressione a tecla “Enter”.

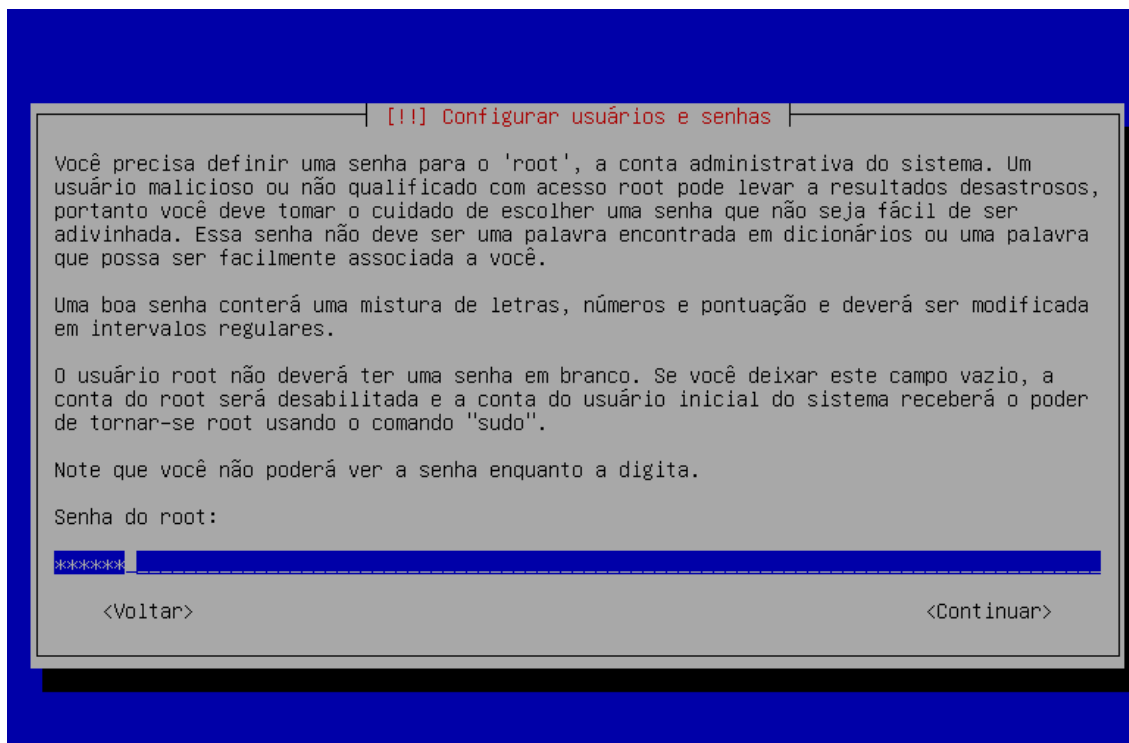


Figura 8 - Configurar usuários e senha

- Confirme a senha de “root” e pressione a tecla “Enter”

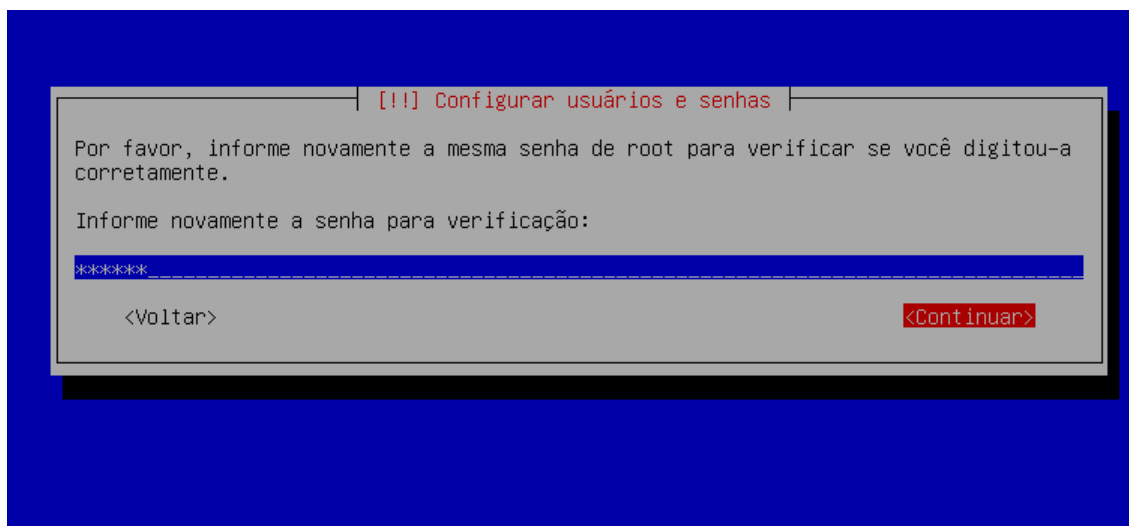


Figura 9 - confirmação de senha

- Na tela a seguir, o usuário deve definir o nome de usuário para sua conta. Esta conta de usuário será criada para a execução de tarefas não administrativas. Tarefas administrativas serão executadas somente com a permissão de “root” (senha definida no passo anterior). Insira o nome desejado e pressione a tecla “Enter”.



[[!]] Configurar usuários e senhas

Uma conta de usuário será criada para você usar no lugar da conta de root para tarefas não-administrativas.

Por favor, informe o nome real deste usuário. Esta informação será usada, por exemplo, como a origem padrão para mensagens enviadas por este usuário bem como por qualquer programa que exiba ou use o nome real do usuário. Seu nome completo é uma escolha razoável.

Nome completo para o novo usuário:

Aker1

<Voltar> <Continuar>

Figura 10 - Nome completo para o novo usuário

- A seguir, defina o nome de usuário. Ao definir o nome de usuário desejado pressione a tecla “Enter”.

[[!]] Configurar usuários e senhas

Informe um nome de usuário para a nova conta. Seu primeiro nome é uma escolha razoável. O nome de usuário deverá ser iniciado com uma letra minúscula, que pode ser seguida de qualquer combinação de números e mais letras minúsculas.

Nome de usuário para sua conta:

aker1

<Voltar> <Continuar>

Figura 11 - Nome de usuário para sua conta

- Defina sua senha de usuário. Ao definir a senha desejada pressione a tecla “Enter”.

[[!]] Configurar usuários e senhas

Uma boa senha conterá uma mistura de letras, números e pontuação e deverá ser modificada em intervalos regulares.

Escolha uma senha para o novo usuário:

<Voltar> <Continuar>

Figura 12 - senha para novo usuário



- Confirme a senha de usuário e pressione a tecla “**Enter**”

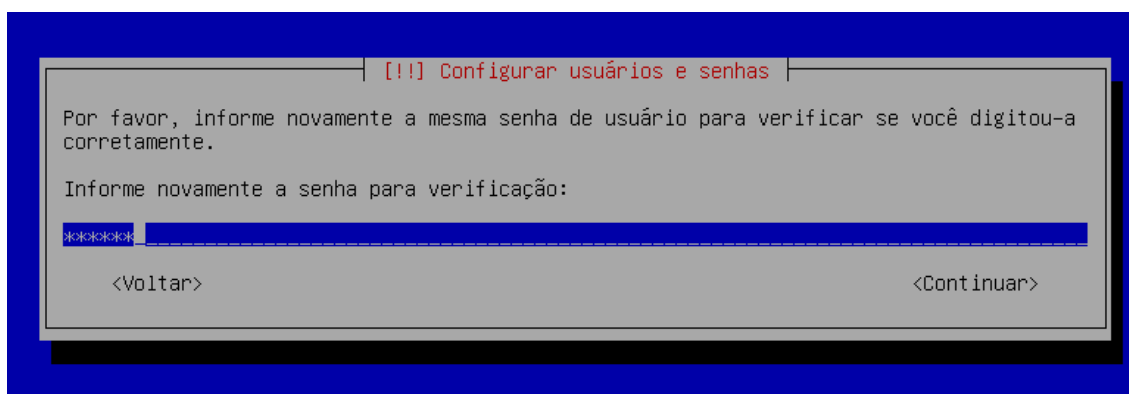


Figura 13 - confirmação de senha

- Em seguida, selecione o estado ou província para definir o fuso horário do sistema do Aker Report Center. Ao definir a localidade desejada pressione a tecla “**Enter**”.

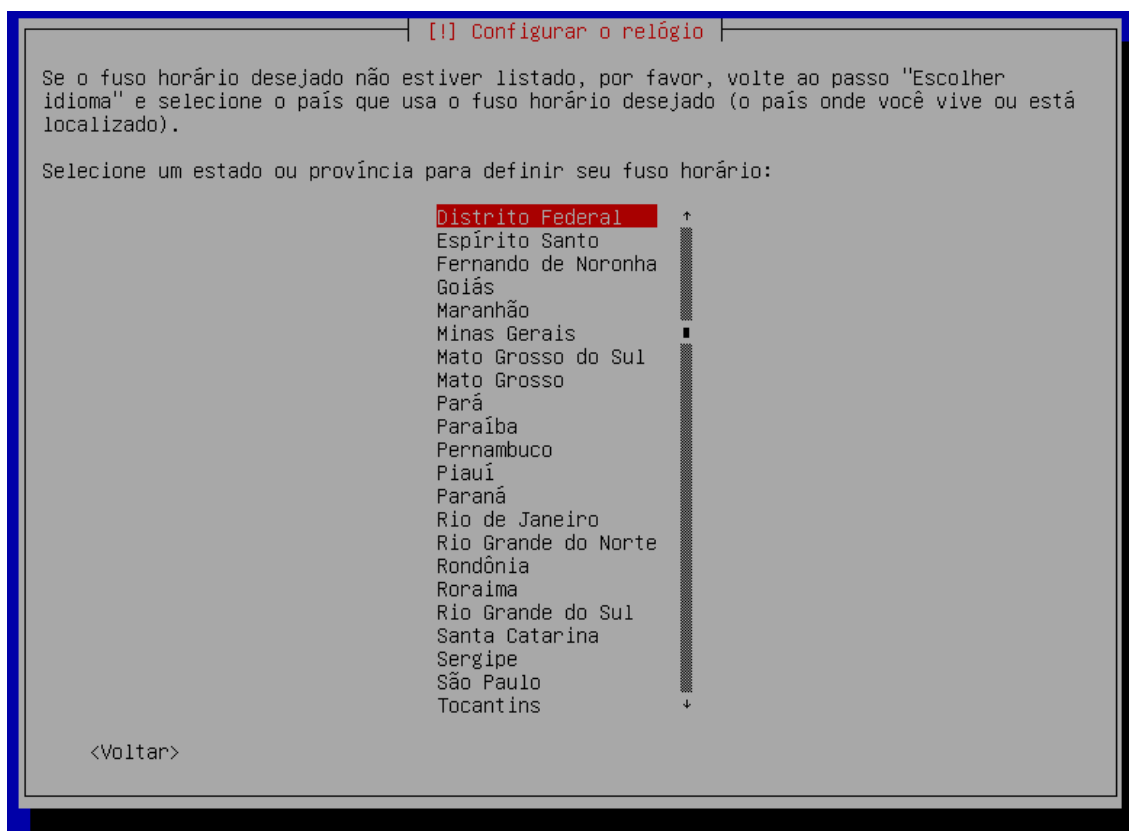


Figura 14 - configuração do relógio

- Em seguida, selecione o método de particionamento que será utilizado no disco. Ao selecionar o método desejado e clique em “**Continuar**”.

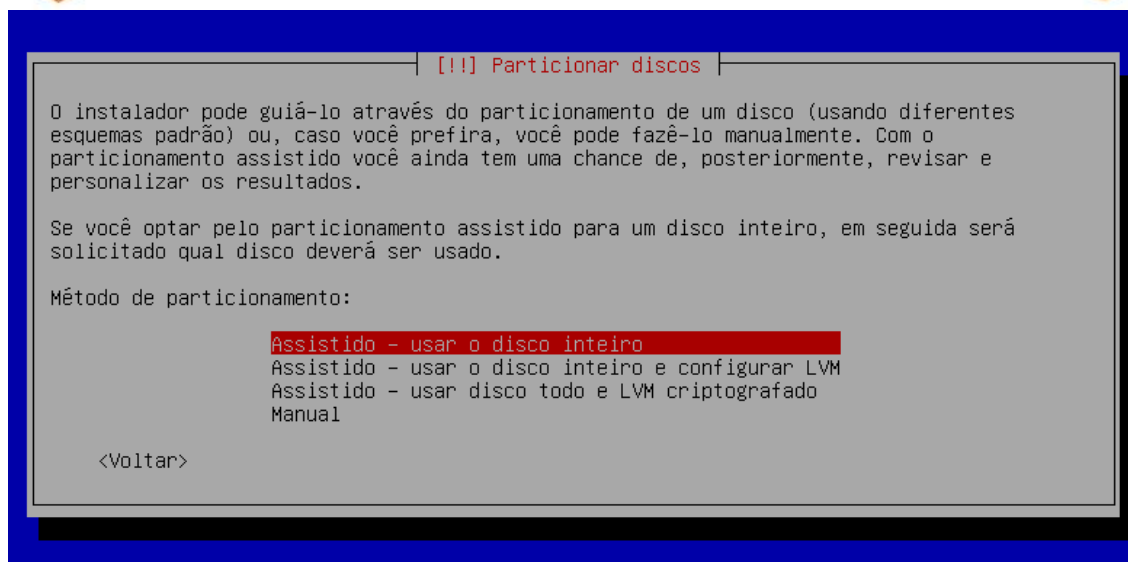


Figura 15 - Particionar discos



É recomendado que o disco seja particionado utilizando a opção **“Assistido – utilizar o disco inteiro e configurar LVM”**.

O LVM faz com que a administração de partições fique mais flexível oferecendo as seguintes vantagens:

- ✓ Redimensionamento de partições em tempo real, ou seja, aumento de tamanho de partições com o sistema operacional em utilização;
 - ✓ Junção de várias Partições;
 - ✓ Junção de vários HDs;
 - ✓ Criação de imagens de backup;
 - ✓ Stripping;
 - ✓ Mirroring;
- Em seguida, selecione o disco que será particionado e pressione a tecla **“Enter”**.

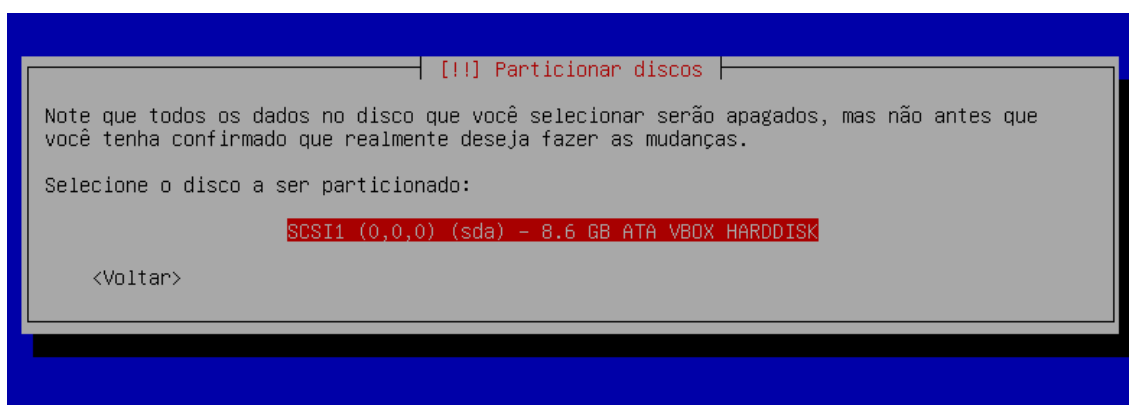


Figura 16 - seleção de disco a ser particionado



- Selecione qual o esquema de particionamento do sistema será utilizado na instalação. Ao definir o esquema de particionamento desejado pressione a tecla “**Enter**”.

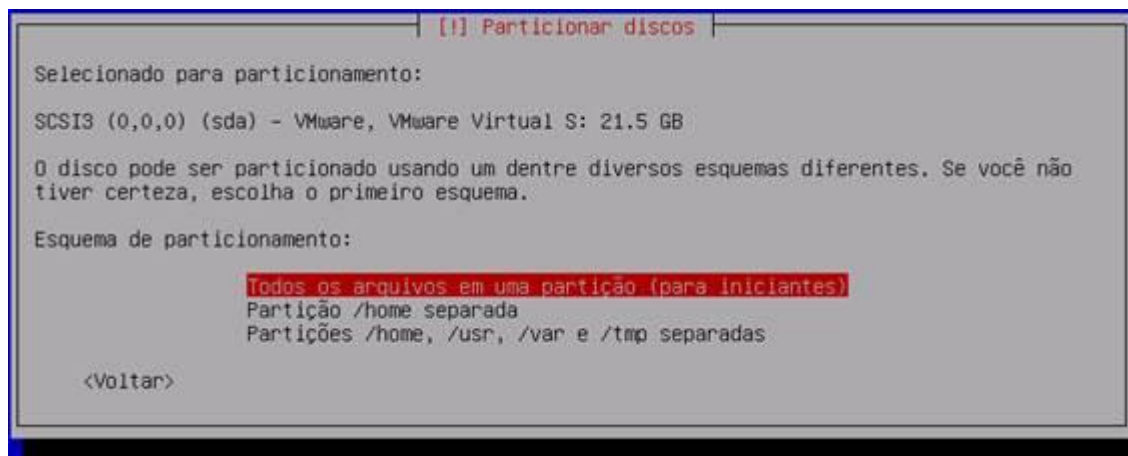


Figura 17 - Esquema de particionamento

- A tela a seguir, exibe as configurações da partição de disco. Ao verificar as informações selecione a opção “**Finalizar o particionamento e escrever as mudanças no disco**” pressione a tecla “**Enter**”.

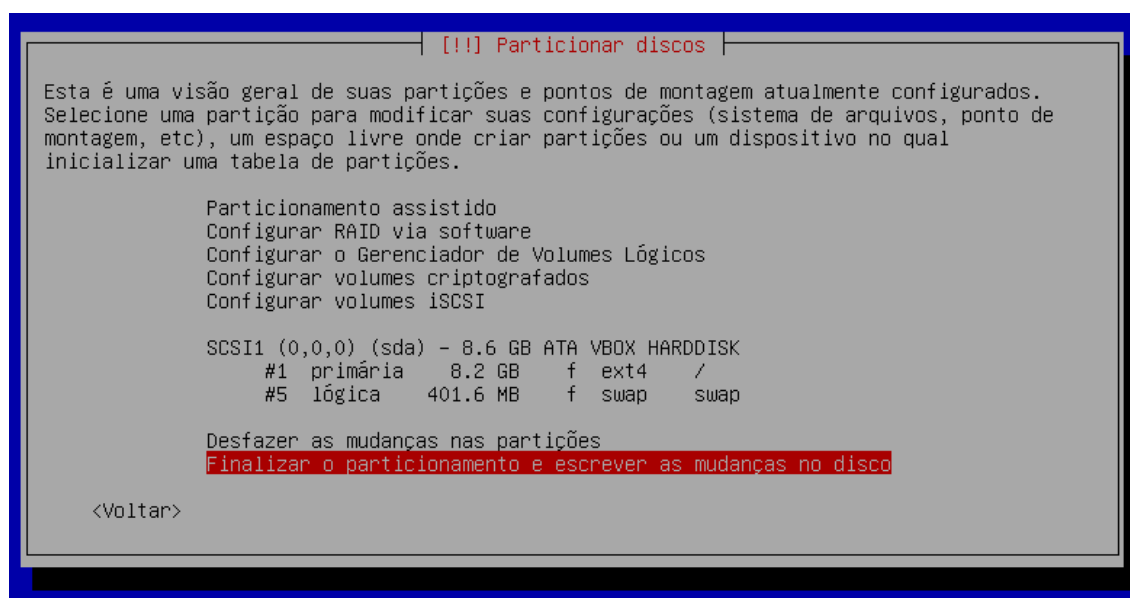


Figura 18 - Finalizar o particionamento e escrever as mudanças no disco

- Confirme se as mudanças exibidas serão ou não escritas no disco. Selecione a opção desejada e pressione a tecla “**Enter**”.

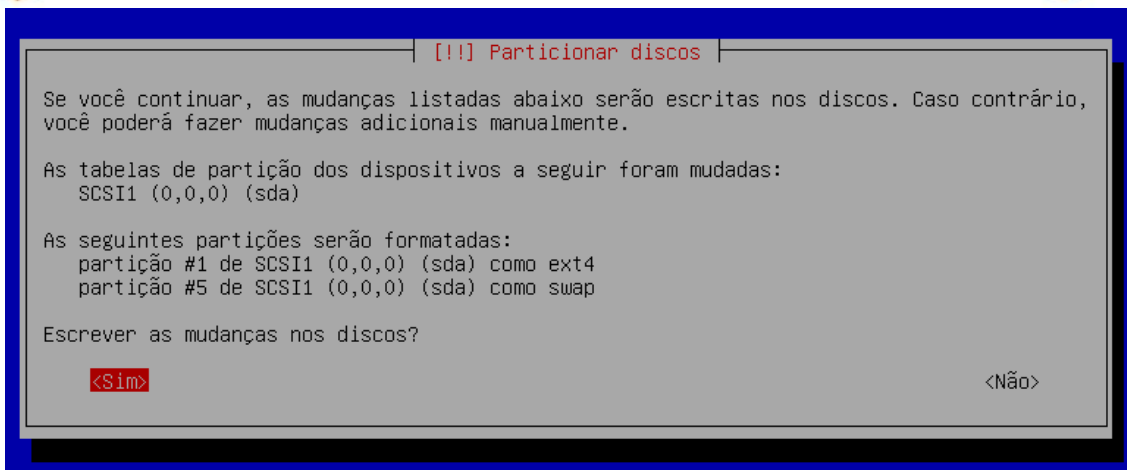


Figura 19 - Confirmação e mudanças

- A instalação será iniciada.

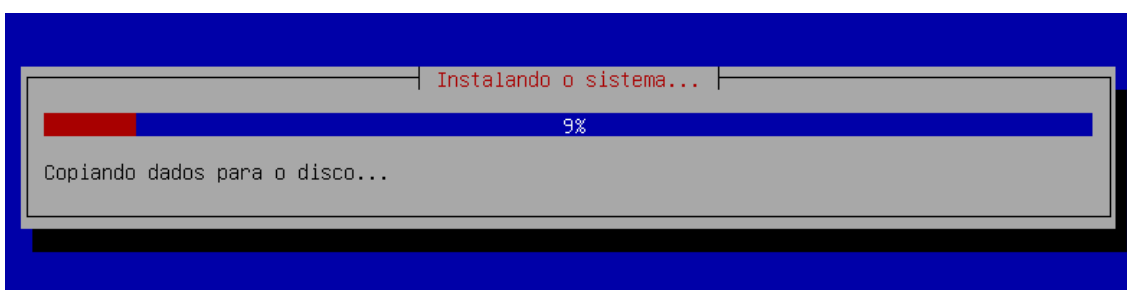


Figura 20 - instalando o sistema

- Em seguida, o usuário deve selecionar se vai ou não *utilizar* um espelho de rede. Selecione a opção desejada e pressione a tecla “**Enter**”.

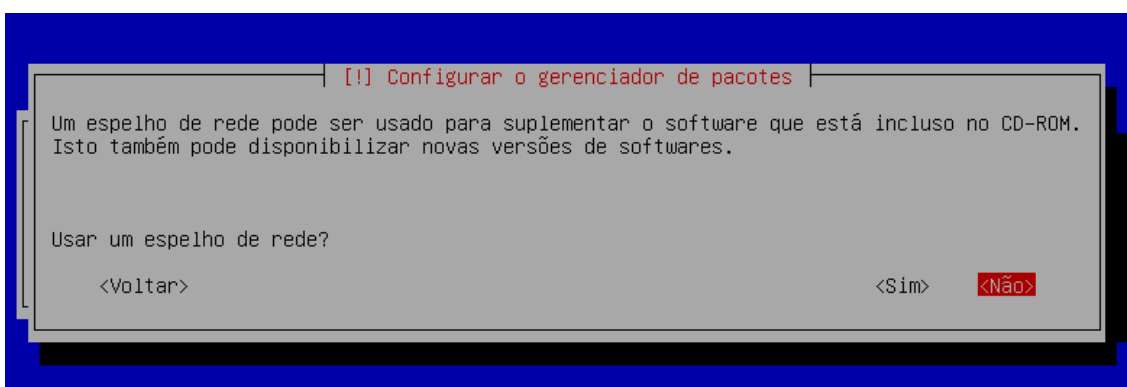


Figura 21 - configurar o gerenciador de pacotes



Figura 22 - configurando o apt

- Na tela a seguir, selecione a opção “**Sim**” para que o carregador de inicialização GRUB seja instalado no registro mestre de inicialização.

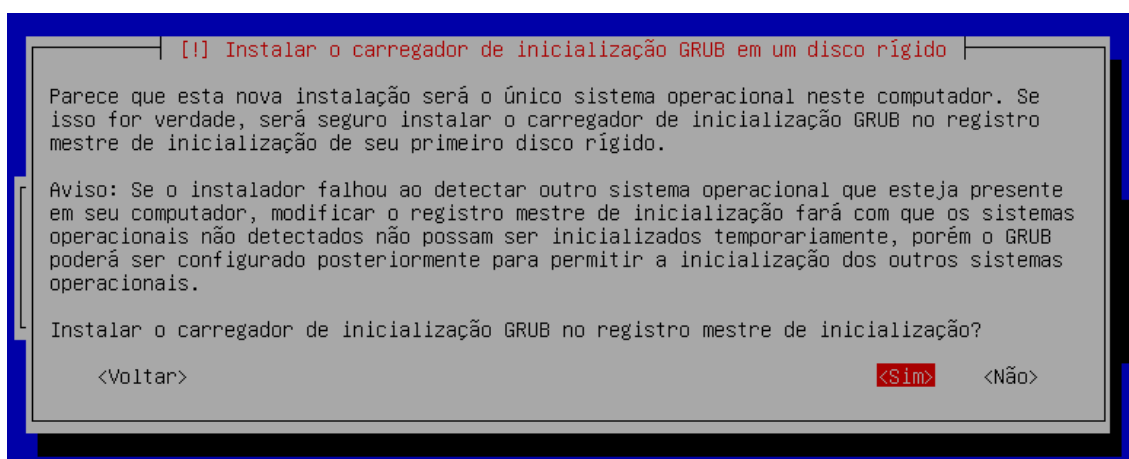


Figura 23 - instalar o carregador de inicialização GRUB

- Selecione o dispositivo que o carregador de inicialização será instalado.

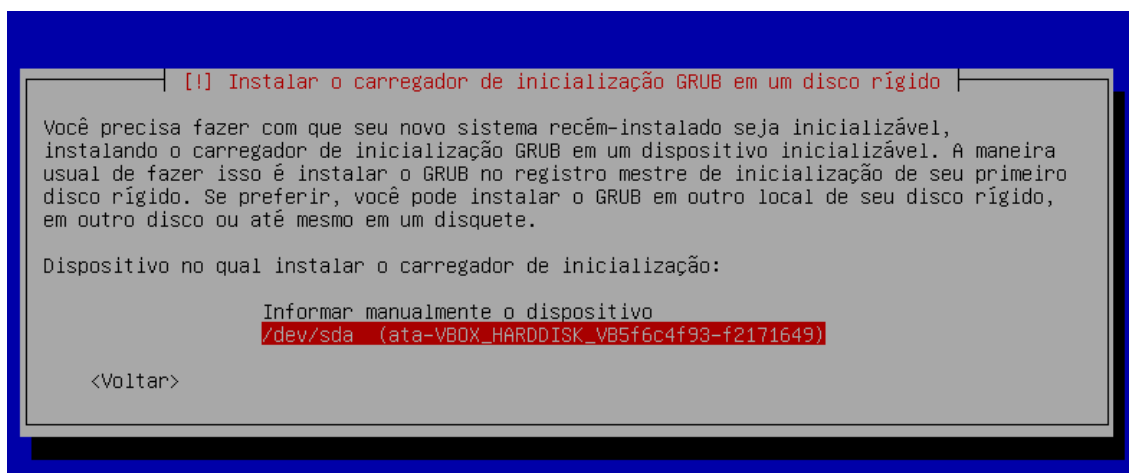


Figura 24 - seleção de dispositivo para instalação do carregador de inicialização

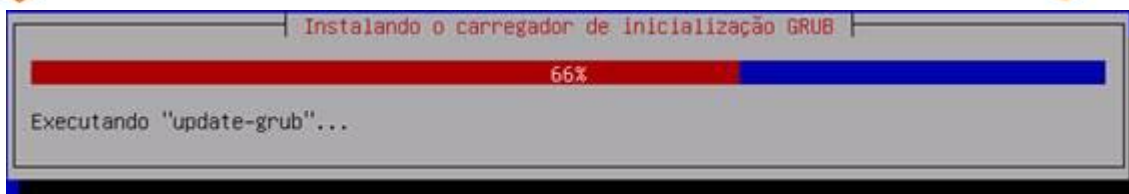


Figura 25 - Instalando o carregador de inicialização GRUB

- A tela a seguir será exibida quando a instalação for concluída. Pressione a tecla “Enter” para reiniciar a máquina e iniciar o sistema do Aker Report Center.

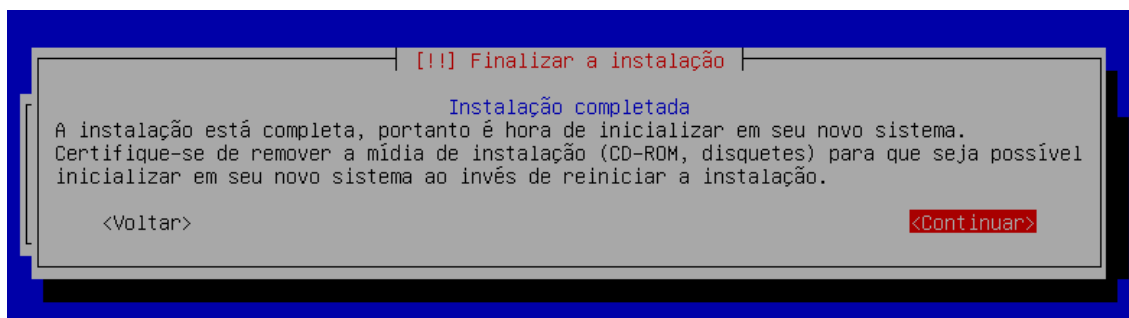


Figura 26 - Finalizar a instalação

Para visualizar o **endereço IP** que foi designado ao seu Aker Report Center, acesse a Interface de texto, e insira o comando “**ifconfig**”, como exibido na imagem abaixo (*Para executar esta operação é necessário estar com permissões de root*):

```
root@AkerReportCenter:/home/aker1# ifconfig
eth0      Link encap:Ethernet  Endereço de HW 08:00:27:5d:e2:a7
          inet end.: 192.168.0.12  Bcast:192.168.0.255  Masc:255.255.255.0
          endereço inet6: fe80::a00:27ff:fe5d:e2a7/64  Escopo:Link
          UP BROADCASTRUNNING MULTICAST  MTU:1500  Métrica:1
          RX packets:64 errors:0 dropped:0 overruns:0 frame:0
          TX packets:76 errors:0 dropped:0 overruns:0 carrier:0
          colisões:0 txqueuelen:1000
          RX bytes:9463 (9.2 KiB)  TX bytes:6956 (6.7 KiB)

lo        Link encap:Loopback Local
          inet end.: 127.0.0.1  Masc:255.0.0.0
          endereço inet6: ::1/128  Escopo:Máquina
          UP LOOPBACKRUNNING  MTU:65536  Métrica:1
          RX packets:6 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6 errors:0 dropped:0 overruns:0 carrier:0
          colisões:0 txqueuelen:0
          RX bytes:300 (300.0 B)  TX bytes:300 (300.0 B)
```

Figura 27 - Visualizando IP para acesso no browser

Digite o IP (**192.168.0.12 no exemplo acima**) em seu navegador para acessar o Aker Report Center.

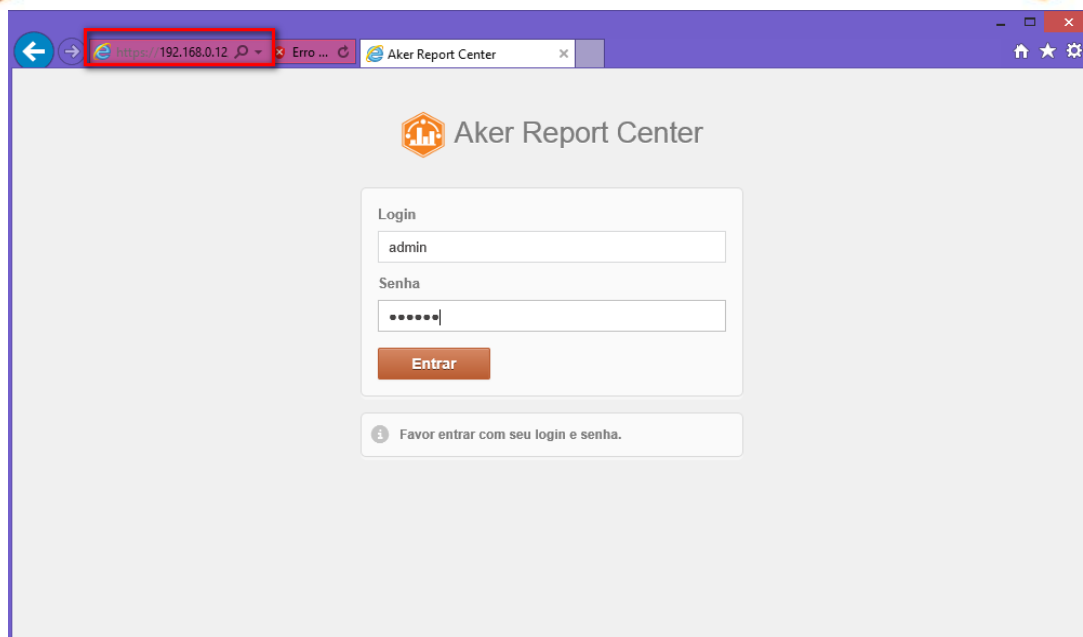


Figura 28 - Acesso web

2.2 Expandindo espaço em disco - LVM

Após adquirir mais espaço em disco, é necessário fazer com que o sistema do Aker Report Center reconheça o espaço adicional, para isso siga os passos abaixo:

- Este processo é usado apenas em Máquinas Virtuais. Por exemplo, o usuário possui uma VM com 100 Gigas de disco, e gostaria de expandir o tamanho do disco para 250 Gigas.

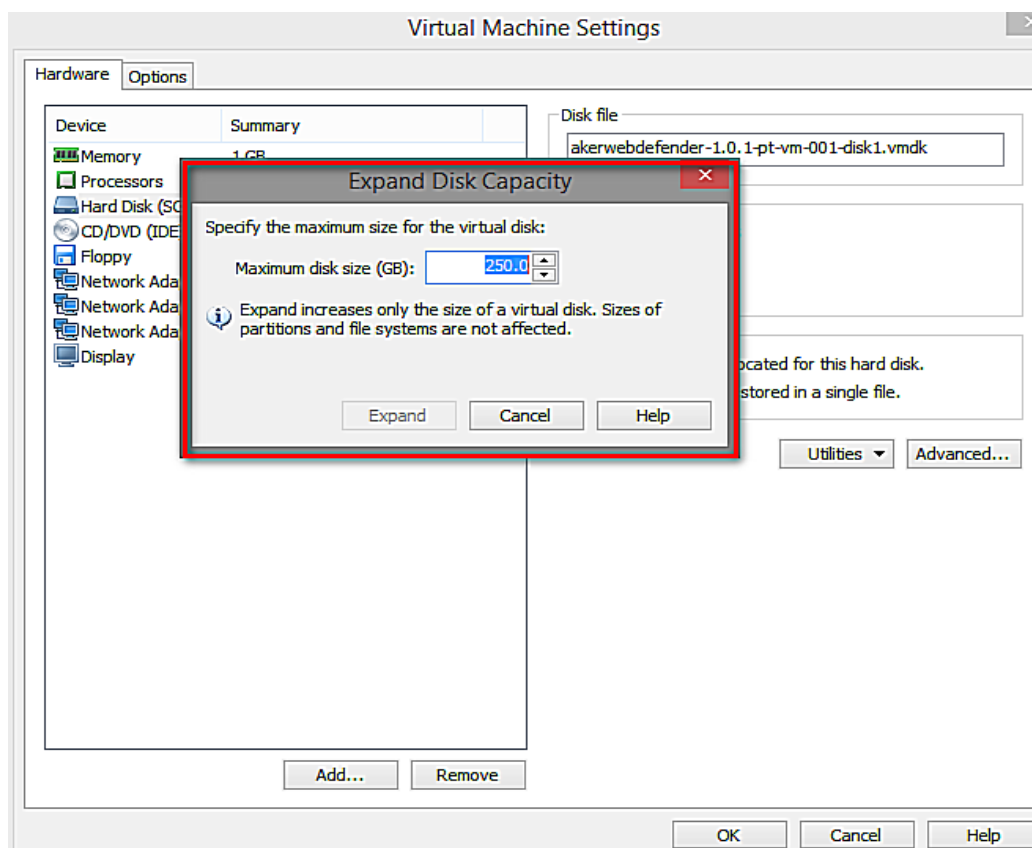


Figura 29 - Expandir a capacidade do disco

**Passo 1**

- ❖ Acesse seu servidor do Aker Report Center via SSH, e digite seu nome de usuário e senha. Em seguida, execute a sequência de comandos:

➤ **# fdisk -l /dev/sda**

1. Anote o valor do último número do cilindro da partição /dev/sda5. **41940991 no exemplo abaixo.**

```
login as: aker
aker@10.4.255.243's password:
Linux reportcenter 3.2.0-4-amd64 #1 SMP Debian 3.2.57-3 x86_64

Bem vindo ao Aker Report Center!

Last login: Thu Sep 25 13:11:02 2014
aker@reportcenter:~$ su
Senha:
root@reportcenter:/home/aker# fdisk -l /dev/sda

Disk /dev/sda: 53.7 GB, 53687091200 bytes
255 heads, 63 sectors/track, 6527 cylinders, total 104857600 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x000dc9de

   Device Boot      Start         End      Blocks    Id  System
/dev/sda1  *        2048       499711       248832    83   Linux
/dev/sda2                501758      41940991      20719617     5   Extended
/dev/sda5                501760      41940991      20719616    8e   Linux LVM
```

Figura 30 - comando fdisk -l /dev/sda

Em seguida entre com o comando exibido abaixo e pressione a tecla 'Enter':

➤ **# fdisk /dev/sda**

2. Em seguida, digite 'N', para inserir uma nova partição.

```
root@reportcenter:/home/aker# fdisk /dev/sda

Command (m for help): n
```

Figura 31 - digite 'N' para inserir uma nova partição

3. Em seguida, digite 'P' e pressione a tecla "Enter", para adicionar uma partição primária.



```

root@reportcenter:/home/aker# fdisk /dev/sda

Command (m for help): n
Partition type:
   p   primary (1 primary, 1 extended, 2 free)
   l   logical (numbered from 5)
Select (default p): p

```

Figura 32 - digite 'p' para adicionar uma partição primária

4. Na opção “número da partição (partition number)”, digite 3 e pressione a tecla “Enter”;

```

Partition number (1-4, default 3): 3
First sector (499712-104857599, default 499712):

```

Figura 33 - definindo o número da partição

5. Digite o número anotado na primeira imagem para que o cilindro se inicie a partir dele.

```

First sector (499712-104857599, default 499712): 41940991
Sector 41940991 is already allocated

```

Figura 34 - definindo o valor para o primeiro setor

6. Para a outra parte do cilindro, será exibido todo o espaço disponível. Pressione a tecla “Enter”.

```

First sector (499712-104857599, default 499712): 41940991
Sector 41940991 is already allocated
First sector (41940992-104857599, default 41940992):
Using default value 41940992
Last sector, +sectors or +size(K,M,G) (41940992-104857599, default 104857599): [Enter]

```

Figura 35 - Informação dos setores

7. Digite ‘P’ para visualizar a nova partição criada, **/dev/sda3**

Device	Boot	Start	End	Blocks	Id	System
/dev/sda1	*	2048	499711	248832	83	Linux
/dev/sda2		501758	41940991	20719617	5	Extended
/dev/sda3		41940992	104857599	31458304	83	Linux
/dev/sda5		501760	41940991	20719616	8e	Linux LVM

Figura 36 - Visualizando a nova partição

8. Digite ‘W’ para salvar e aplicar as alterações no disco;



Uma mensagem de “**WARNING**” será exibida, informando que as alterações serão aplicadas somente após a reinicialização.

```
Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.

WARNING: Re-reading the partition table failed with error 16: Dispositivo ou recurso está ocupado.
The kernel still uses the old table. The new table will be used at
the next reboot or after you run partprobe(8) or kpartx(8)
Syncing disks.
```

Figura 37 - mensagem de Warning

9. Em seguida reinicie o servidor com o comando '**reboot**', para que o sistema reconheça as novas partições;

```
root@reportcenter:/home/aker# reboot

The system is going down for reboot NOW! (pts/0) (Thu Sep 25 17:24:51 2014):
root@reportcenter:/home/aker#
```

Figura 38 – Reiniciando a máquina para aplicar as mudanças

Passo 2

Após reiniciar a máquina, será necessário adicionar as partições ao LVM, para isso execute os comandos abaixo:

1. Crie a nova partição no LVM executando o comando abaixo;

Pvcreate /dev/sda3

```
root@reportcenter:/home/aker# pvcreate /dev/sda3
Writing physical volume data to disk "/dev/sda3"
Physical volume "/dev/sda3" successfully created
root@reportcenter:/home/aker#
```

Figura 39 - comando para cria uma nova partição no LVM

2. Agora, deve-se expandir o *Volume do Aker Report Center* adicionando o "sda3", para isso use o comando abaixo;

Vgextend reportcenter /dev/sda3

```
root@reportcenter:/home/aker# vgextend reportcenter /dev/sda3
Volume group "reportcenter" successfully extended
root@reportcenter:/home/aker#
```

Figura 40 - comando para expandir o volume do Aker Report Center

3. Expansão do volume lógico da LVM com o valor contratado;



```
root@reportcenter:/home/aker# lvextend -l +100%FREE /dev/reportcenter/root
Extending logical volume root to 49,01 GiB
Logical volume root successfully resized
root@reportcenter:/home/aker#
```

Figura 41 – comando utilizado para expandir o volume lógico da LVM



Supondo que a VM se chame Aker Report Center e o volume lógico a ser expandido se chama root, o parâmetro “-l +100%FREE” deve ser usado para utilizar todo o espaço disponível para expansão.

4. Use o comando abaixo para redimensionar o sistema de arquivos da partição /reportcenter/root;

```
root@reportcenter:/home/aker# resize2fs /dev/reportcenter/root
resize2fs 1.42.5 (29-Jul-2012)
Filesystem at /dev/reportcenter/root is mounted on /; on-line resizing required
old_desc_blocks = 2, new_desc_blocks = 4
Performing an on-line resize of /dev/reportcenter/root to 12847104 (4k) blocks.
The filesystem on /dev/reportcenter/root is now 12847104 blocks long.
```

Figura 42 - comando para redimensionar o sistema de arquivos

5. Reinicie o servidor do Aker Report Center novamente para finalizar o processo;

```
root@reportcenter:/home/aker# reboot

The system is going down for reboot NOW! (pts/0) (Thu Sep 25 17:24:51 2014):
root@reportcenter:/home/aker#
```

Figura 43 - reiniciar o sistema para aplicar as alterações

Ao reiniciar, o espaço expandido no disco será reconhecido e já conseguirá ser utilizado.

2.3 Licenciamento

Ao concluir a instalação do sistema Aker Report Center, o usuário deve acessar o endereço designado para o Aker Report Center em seu navegador, e utilizar o nome de usuário e senha exibidos a seguir para efetuar o login no sistema **(a interface de rede é configurada por padrão em modo DHCP)**.

- Senha padrão Interface texto

Usuário padrão SSH: aker

Senha padrão SSH: 123456

- Senha padrão Interface remota



Usuário padrão: admin

Senha padrão: 123456



O número máximo de tentativas para logar-se no **Aker Report Center** são 3, caso o usuário exceda este número máximo de tentativas, terá que esperar 2 minutos para tentar efetuar o login novamente.

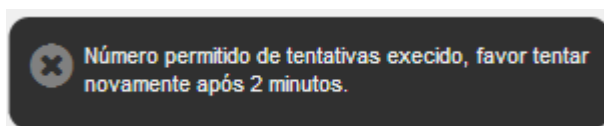


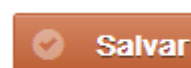
Figura 44 - Mensagem ao errar a senha mais de 3 vezes

Figura 45 - Tela de login

No primeiro login o usuário deve gerar a chave de licenciamento do produto. Ao gerar a chave de licenciamento o usuário deve enviar esta chave para licenca@aker.com.br solicitando sua licença.

Para gerar a chave de licenciamento do produto e carregar a licença do produto siga os passos abaixo:

- Preencha o campo “Licenciado para” e clique em





Gerar chave

Licenciado para

aker

Chave

8CC6-9480-8162-C97E



Salvar



Remover chave



Aplicar licença



Voltar

Figura 46 - Gerar chave

Licenciando para: Neste campo deve-se informar o nome do usuário ou empresa para qual o produto está sendo licenciado.

Chave: Ao preencher o campo “Licenciado para” e clicar em “**Salvar**” fará com que uma chave de licenciamento seja gerada automaticamente. O usuário deve encaminha esta chave para licenca@aker.com.br solicitando sua licença. Ao receber a licença siga os passos a seguir *(ao enviar a solicitação o usuário receberá sua licença no período máximo de 24h).*

- Ao receber a licença clique em



Aplicar licença

- Na janela Aplicar Licença clique no ícone  para localizar sua licença.

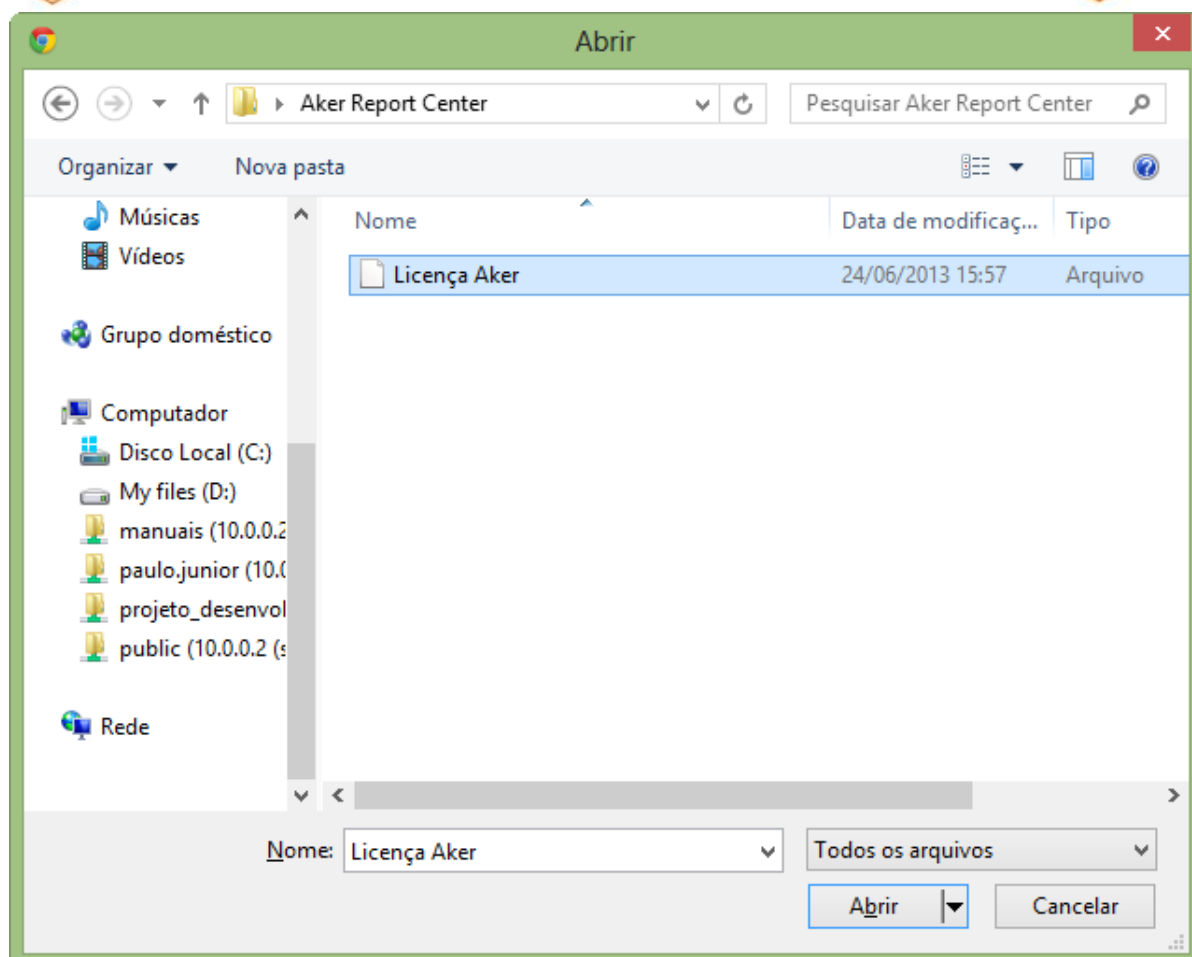


Figura 47 - Localizando licença



Figura 48 - Opções de carregamento da licença

- Ao localizar o arquivo clique no ícone  para carregar o arquivo. Ao carregar a licença suas informações serão exibidas na mesma tela como na imagem a seguir:



✓ Aplicar Licença

Informações da Licença

Nome	aker
Serial	200000020697
Data de expiração	30/01/2014
Nº de ativos	20
Quantidade de eventos	250.000.000

Figura 49 - Informação da licença

Após carregar a licença, serão exibidas as informações sobre sua licença:

Nome: Neste campo é exibido o nome do titular da licença;

Serial: Neste campo é exibido o serial da licença em uso/carregada;

Data de expiração: Neste campo é exibido a data de expiração da licença em uso/carregada;

Nº de ativos: Neste campo é exibido o número de ativos suportados pela licença em uso/carregada ativo para a licença em questão;

Quantidades de eventos: Neste campo é exibido a quantidade de eventos suportados pela licença em uso;



Esta janela permite que o usuário visualize as informações da licença em uso, lembrando que ao carregar uma nova licença as informações serão atualizadas, desta forma, somente as informações da licença em uso serão exibidas.

Depois de completar o processo de upload da licença no sistema, serão exibidas as informações da licença, clique no botão  depois do upload para completar processo de licenciamento.



O sistema enviará mensagens automáticas de notificação para o cliente, quando o número máximo de eventos suportado pela licença em questão estiver próximo de ser atingido. Quando a licença se expirar o Aker Report Center não irá gerar relatórios, mas todos os logs recebidos serão armazenados. Ao regularizar a licença os logs armazenados serão tratados e o usuário conseguirá gerar relatórios com estes logs.



O Aker Report Center possui 5 (cinco) menus principais que facilitam o gerenciamento do administrator. Estes menus serão abordados nos capítulos a seguir.

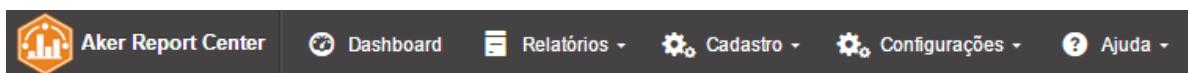


Figura 50 - Menus

Dashboard



3 Dashboard

Este capítulo mostra o que é, e para que serve o Dashboard do Aker Report Center.

O Dashboard do Aker Report Center foi projetado para oferecer maior transparência e facilidade no controle dos dados mais relevantes para sua empresa, auxiliando os administradores do Aker Report Center na gestão dos logs

O Dashboard possui 4 (quatro abas) que serão abordadas nas páginas a seguir:

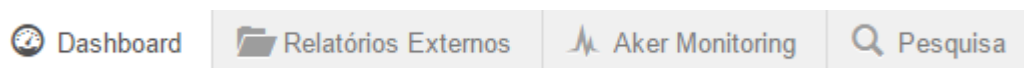


Figura 51 - Abas do Dashboard

3.1 *Aba Dashboard*

A aba Dashboard oferece transparência e facilidade no controle de dados para os gestores do Aker Report Center, permitindo que os mesmos possam configurar os Widgets de acordo com a necessidade de sua empresa. Resumindo os dados mais importantes de uma entidade e seus respectivos ativos exibindo os dados nas mais diversas opções de gráficos disponíveis.

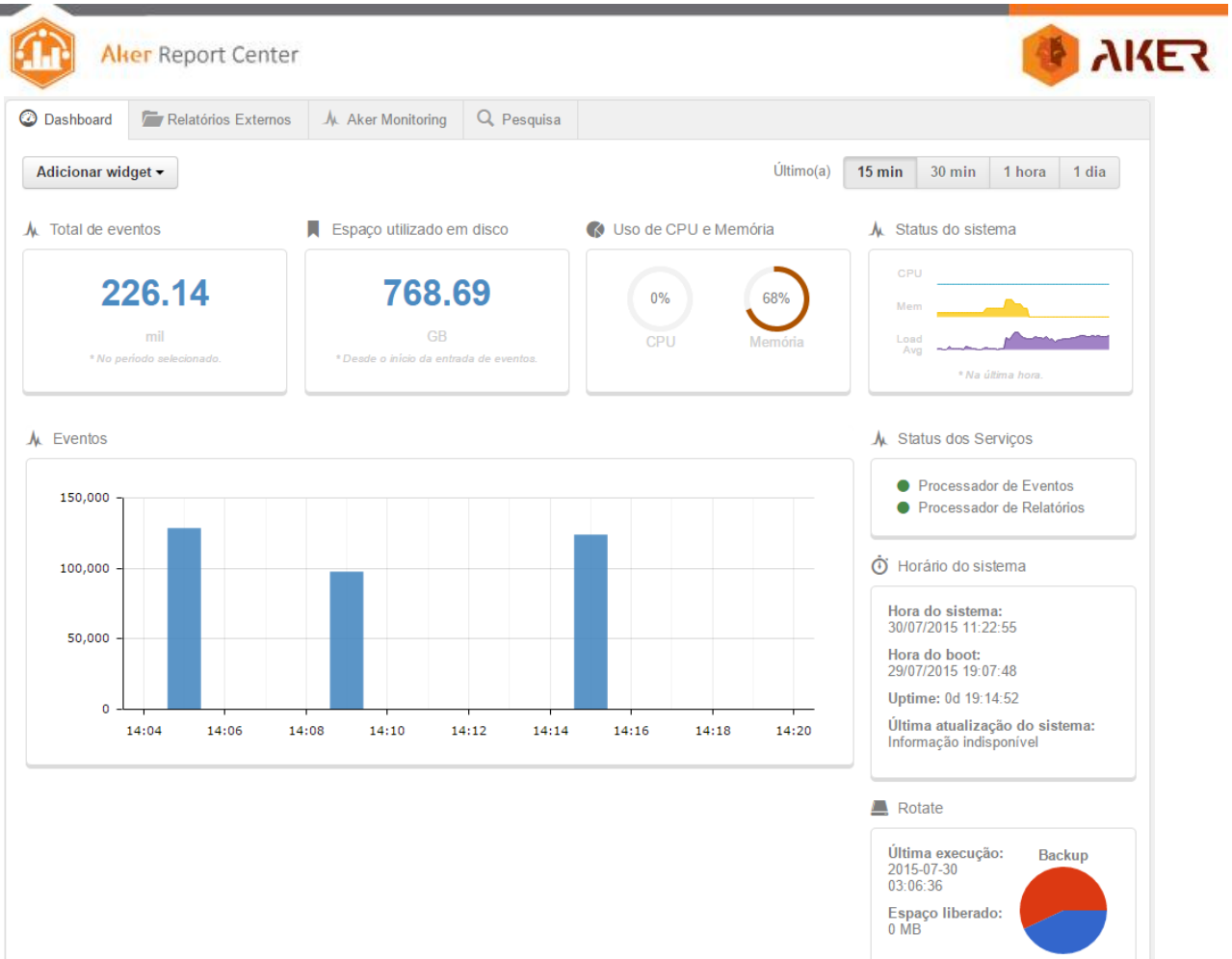


Figura 52 - Aba Dashboard

Na aba Dashboard existe um Widget que é atualizado em tempo real, este é o Widget “Uso de CPU e Memória”.

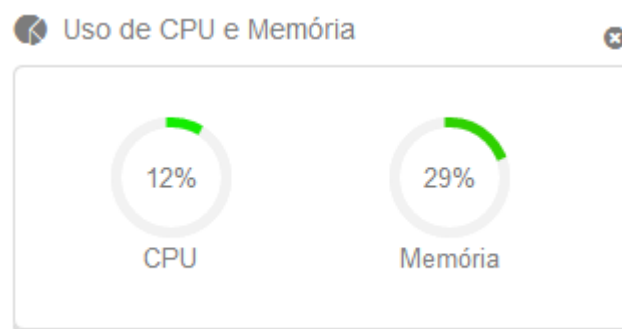


Figura 53 – Widget “Uso de CPU e Memória” atualizado em tempo real

O Widget “**Total de eventos**” exibe a quantidade de eventos de acordo com o período selecionado. As opções são: **últimos 15 minutos**, **últimos 30 minutos**, **Última hora**, **Último dia**.



Figura 54 – Widget “Total de eventos”

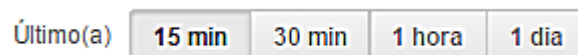


Figura 55 - Opções de período

E o Widget “**Espaço utilizado em disco (eventos)**” exibe o espaço utilizado em disco desde o início do recebimento de eventos do sistema.



Figura 56 - Widget "espaço utilizado em disco"

Os Widgets abordados acima “**Total de eventos, Espaço utilizado em disco, e Uso de CPU e Memória**” são as únicas exceções de configuração dos Widgets. Os demais Widgets são atualizados de forma consolidada a cada 5 minutos.

Ativos
Eventos
Eventos / Prioridade
Últimos Eventos
Fila de relatórios

Figura 57 - Opções de Widget



3.2 Aba Relatórios Externos

Nesta aba o usuário pode ter acesso a todos os relatórios prontos, que foram enviados por outros ativos via FTP (por exemplo, o Aker Firewall).



Para que um ativo tenha a permissão para enviar relatórios prontos para outros ativos, é necessário configurar o mesmo. Na janela do ativo, selecione “**Sim**” para a opção “**Este ativo envia relatórios prontos**”. Para mais informação sobre cadastro de ativos veja o capítulo “[Cadastrando um novo ativo](#)”

Este ativo envia relatórios prontos? ☒ Sim ☐ Não

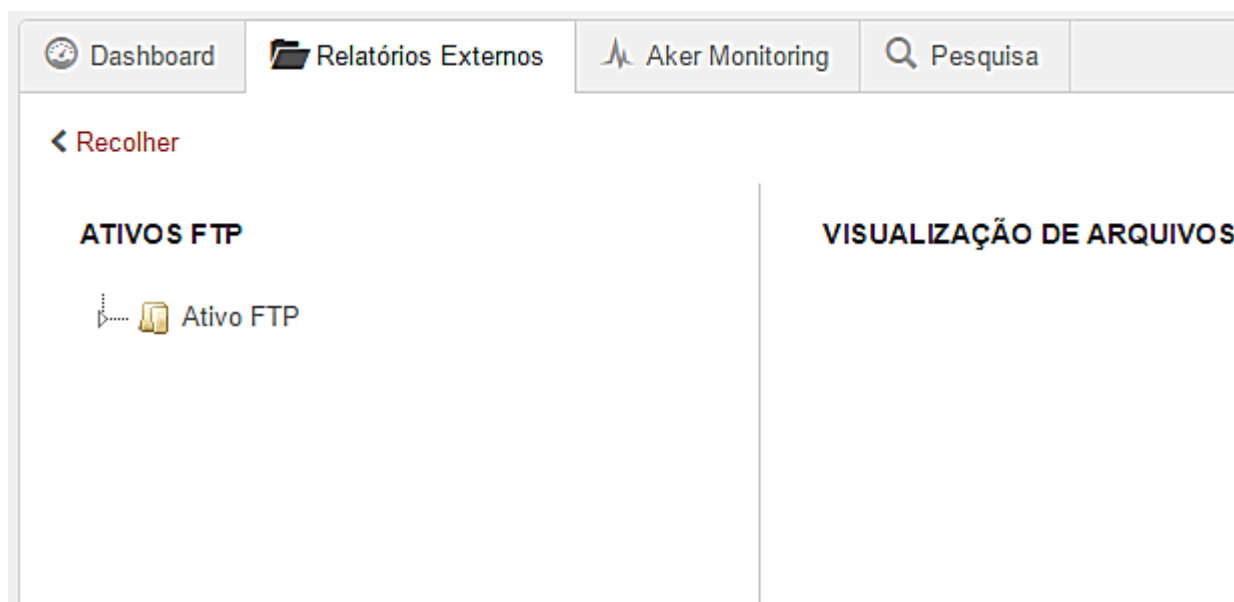


Figura 58 - Relatórios Recebidos

Ativos FTP

Nesta parte da aba de *Relatórios Recebidos* é exibido a lista de relatórios que foram recebidos por outros ativos.



ATIVOS FTP

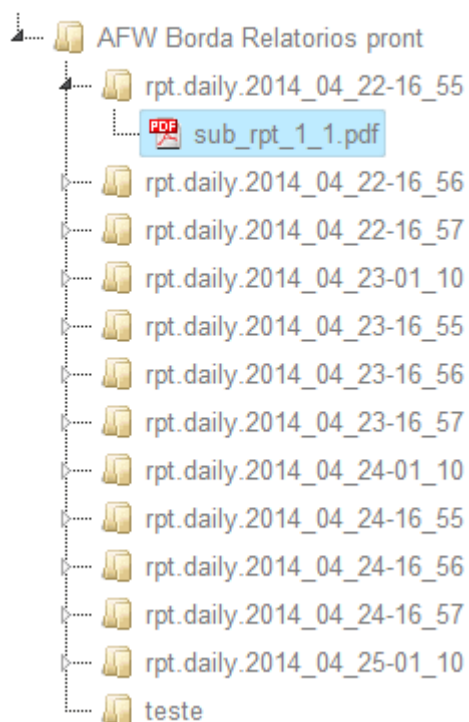


Figura 59 - Ativos FTP

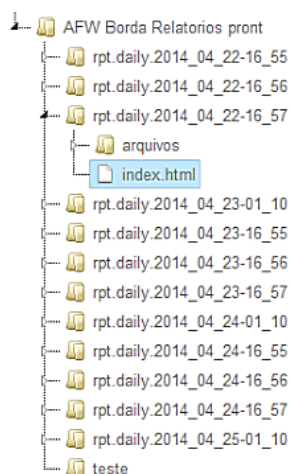
Visualização de arquivos

Nesta parte da aba de *Relatórios Externos*, o usuário pode visualizar o relatório desejado com as informações definidas para o relatório em questão, como: Gráficos, Acessos, Contabilização de tráfego e etc.



< Recolher

ATIVOS FTP



ARQUIVO: INDEX.HTML

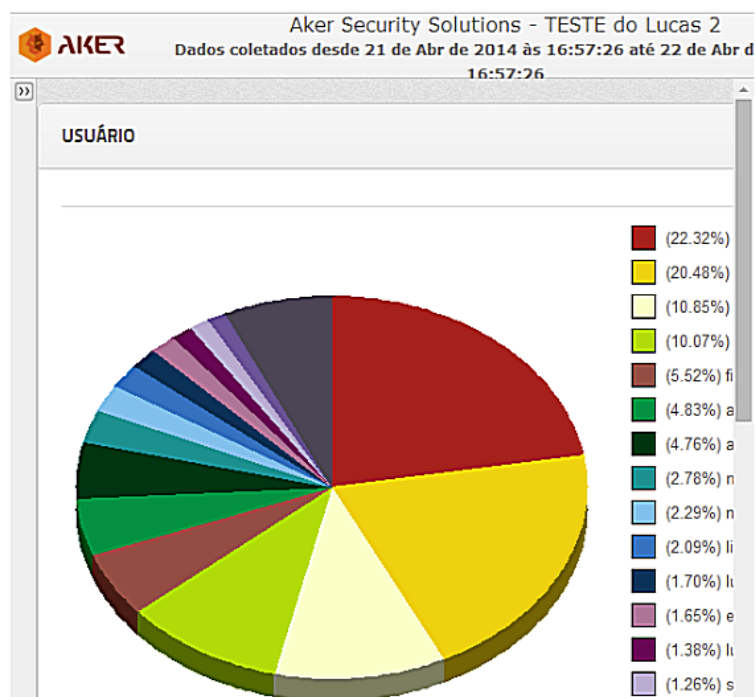


Figura 60 - Visualização de arquivos

3.3 Aba Aker Monitoring

A aba Aker Monitoring permite que o usuário efetue um monitoramento especializado nos ativos, além de um fácil e prático gerenciamento integrado do seu ambiente tecnológico.

Por meio desta aba o usuário tem acesso em tempo real, ao sistema de monitoramento de ativos de rede, como: Servidores, Roteadores, Switches, Firewalls, e banco de dados SQL.

O Aker Monitoring Service envia todos os alertas para o centro de gerenciamento de redes da Aker, que acionará um analista técnico para solucionar os problemas detectados nos ativos de sua rede (*além de enviar e-mails ou SMS ao detectar um problema*).

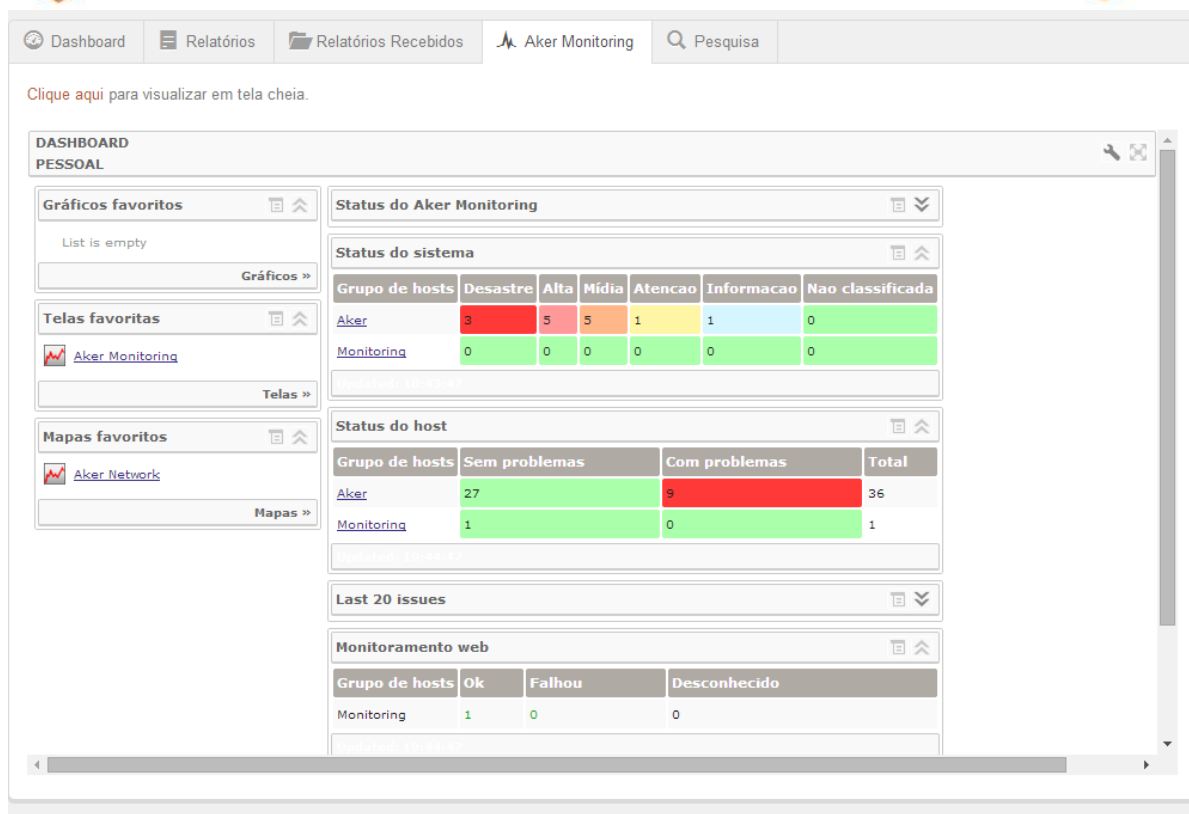


Figura 61 - Aker Monitoring

3.4 Aba Pesquisa

A aba pesquisa permite que o usuário realize pesquisa de valores (*Nomes de usuários, palavras, etc.*) diretamente nos logs armazenados.

- **Ativo:** ativo em que a pesquisa será realizada; (*no exemplo abaixo: Firewall Borda*)
- **Não identificados:** Definir se os logs os quais não forem reconhecidos pelo *Aker Report Center* serão exibidos na pesquisa. Selecionando a opção "**Não identificados**" fará com que dados não reconhecidos sejam exibidos na pesquisa.
- **Valor:** nome que será pesquisado; (*no exemplo abaixo: @gmail.com*)
- **Período:** data que a pesquisa será realizada



No campo ativo o usuário pode filtrar um ativo específico ou realizar a pesquisa em todos os ativos disponíveis. Não é mandatório selecionar as duas datas do período, podendo assim, selecionar uma data ou outra.

FW Homologaçã... ☐ Não identificados @gmail.com 25/04/2014 01:05 25/04/2014 23:35 Pesquisar

Figura 62 - Aba Pesquisa



Q Pesquisa

Firewall Borda

☐ Não identificados

paulo.junior

01/04/2014 11:50

24/04/2014 06:30

Pesquisar

```
1. {date: 22/04/2014 19:33:18, sensor_hostname: matriz.aker.com.br, logtype: Sessao de perfil de acesso
estabelecida, perfil: Padrao, src_ip: 10.0.0.163, username: paulo.junior/radius_pptp, priority: info,
facility: local1},

2. {date: 22/04/2014 19:33:22, sensor_hostname: matriz.aker.com.br, logtype: URL aceita,
site: http://www.msftncsi.com/, url: http://www.msftncsi.com/ncsi.txt, dst_ip: 204.93.33.16, src_ip: 10.0.0.163,
perfil: Padrao, username: paulo.junior/radius_pptp, priority: info, facility: local1},

3. {date: 22/04/2014 19:33:22, sensor_hostname: matriz.aker.com.br, logtype: Contabilidade de trafego HTTP,
site: http://www.msftncsi.com/, url: http://www.msftncsi.com/ncsi.txt, download: 179,
username: paulo.junior/radius_pptp, times: 0.474, upload: 97, priority: info, facility: local1},

4. {date: 22/04/2014 19:33:29, sensor_hostname: matriz.aker.com.br, logtype: Contabilidade de trafego HTTP,
site: http://aupl.ds.download.windowsupdate.com/,
url: http://aupl.ds.download.windowsupdate.com/d/msdownload/update/software/crup/2014/02/windows8.1-kb2919,
download: 5791, username: paulo.junior/radius_pptp, times: 0.53, upload: 355, priority: info, facility: local1},

5. {date: 22/04/2014 19:33:29, sensor_hostname: matriz.aker.com.br, logtype: URL aceita,
site: http://aupl.ds.download.windowsupdate.com/,
url: http://aupl.ds.download.windowsupdate.com/d/msdownload/update/software/crup/2014, dst_ip: 64.211.144.42,
```

Figura 63 - Resultado da pesquisa

Relatórios



AKER

4 Relatórios

Este capítulo mostra como configurar o agendamento, geração de relatórios, e as opções de visualização da fila de relatórios.

Por meio do menu **“Relatórios”** o usuário pode gerar novos relatórios, visualizar a fila de relatórios com o progresso (%), data e o usuário que gerou um relatório específico. Além de ter acesso a todos os relatórios gerados pelo Aker Report Center, configurar e visualizar o agendamento de relatórios.

A seguir mais detalhes sobre as opções deste menu.

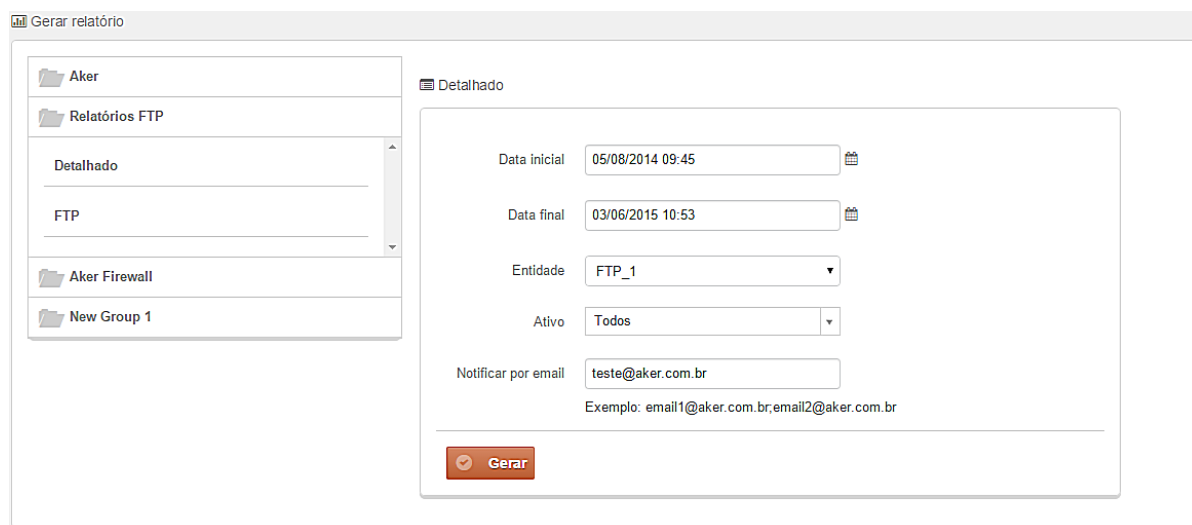


Figura 64 - Opções do menu Relatórios

4.1 Gerar Relatório

Por meio desta janela o usuário pode gerar relatórios pre-configurados de forma prática e rápida. Os relatórios são agrupados em seus respectivos grupos facilitando a pesquisa do usuário.

- É mandatório o preenchimento dos campos **“Data inicial e Data final”** na geração de relatórios.



Gerar relatório

Detalhado

Data Inicial: 05/08/2014 09:45

Data final: 03/06/2015 10:53

Entidade: FTP_1

Ativo: Todos

Notificar por email: teste@aker.com.br

Exemplo: email1@aker.com.br;email2@aker.com.br

Gerar

Figura 65 - gerar relatório



4.2 Fila de Relatórios

Por meio desta janela o usuário pode visualizar todas as solicitações de criação de relatórios, nome do usuário que efetuou a solicitação, data de envio e progresso da criação dos relatórios. Além de visualizar os últimos **20** relatórios completos (*para visualizar todos os relatórios gerados no sistema, acesse o menu [Relatórios gerados](#)*).

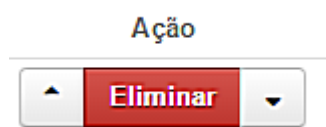
Fila de relatórios				
Relatório	Responsável	Data de envio	Progresso	Ação
Detalhes de acessos a sites	Administrador	23/07/2015 09:36	57%	Eliminar
Sites acessados por usuário	Administrador	23/07/2015 09:36	Pendente	Eliminar
Volume de download por URL	Administrador	23/07/2015 09:36	Pendente	Eliminar
Tempo de navegação por site	Administrador	23/07/2015 09:36	Pendente	Eliminar
Volume de upload por URL	Administrador	23/07/2015 09:36	Pendente	Eliminar
Sites rejeitados por usuário	Administrador	23/07/2015 09:36	Pendente	Eliminar
Top 10 IPs de destino mais acessados	Administrador	23/07/2015 09:36	Pendente	Eliminar
Top 10 serviços por protocolo TCP	Administrador	23/07/2015 09:37	Pendente	Eliminar
Top 10 serviços por protocolo UDP	Administrador	23/07/2015 09:37	Pendente	Eliminar
Top 10 IPs de origem por serviço	Administrador	23/07/2015 09:37	Pendente	Eliminar
Top 10 serviços	Administrador	23/07/2015 09:37	Pendente	Eliminar
Top 10 sites	Administrador	23/07/2015 09:37	Pendente	Eliminar
Top 10 sites rejeitados	Administrador	23/07/2015 09:37	Pendente	Eliminar
Top 10 sites rejeitados por usuário	Administrador	23/07/2015 09:37	Pendente	Eliminar
Top 10 sites por IP de origem	Administrador	23/07/2015 09:37	Pendente	Eliminar
Top 10 sites por usuário	Administrador	23/07/2015 09:38	Pendente	Eliminar
Top 10 conexões TCP	Administrador	23/07/2015 09:38	Pendente	Eliminar
Top 10 usuários com mais download e upload	Administrador	23/07/2015 09:38	Pendente	Eliminar
Top 10 usuários por tempo de tráfego	Administrador	23/07/2015 09:38	Pendente	Eliminar
Top 10 categorias	Administrador	23/07/2015 09:38	Pendente	Eliminar
Top 10 conexões UDP	Administrador	23/07/2015 09:38	Pendente	Eliminar

Figura 66 - Fila de relatórios

Top 10 sites por usuário	Administrador	03/06/2015 15:08	Completo!
Top 10 usuários com mais download e upload	Administrador	03/06/2015 15:08	Completo!
Top 10 sites por IP de origem	Administrador	03/06/2015 15:06	Completo!
Top 10 sites rejeitados por usuário	Administrador	03/06/2015 15:06	Completo!
Top 10 sites rejeitados	Administrador	03/06/2015 15:05	Completo!
Top 10 sites	Administrador	03/06/2015 15:04	Completo!
Top 10 serviços	Administrador	03/06/2015 15:04	Completo!
Top 10 IPs de origem por serviço	Administrador	03/06/2015 15:00	Completo!
Top 10 conexões UDP	Administrador	03/06/2015 14:56	Completo!
Top 10 conexões TCP	Administrador	03/06/2015 14:54	Completo!
Top 10 IPs de destino mais acessados	Administrador	03/06/2015 14:52	Completo!
Sites rejeitados por usuário	Administrador	03/06/2015 14:50	Completo!
Volume de upload por URL	Administrador	03/06/2015 14:49	Completo!
Tempo de navegação por site	Administrador	03/06/2015 14:48	Completo!
Volume de download por URL	Administrador	03/06/2015 14:47	Completo!
Sites acessados por usuário	Administrador	03/06/2015 14:47	Completo!
Detalhes de acessos a sites	Administrador	03/06/2015 14:46	Completo!
Requisições por IP de origem e destino	Administrador	03/06/2015 14:45	Completo!
Quantidade de requisições IP origem/destino	Administrador	03/06/2015 14:45	Completo!
Eventos por Tipo de Log	Administrador	03/06/2015 14:44	Completo!

Figura 67 - Relatórios gerados

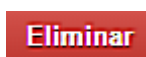
É possível mudar a prioridade da criação de um relatório específico por meio das setas na coluna “Ação”.



Esta seta move o relatório em questão para o topo da fila de geração de relatórios.



Esta seta move o relatório em questão para o fim da fila de geração de relatórios.



Este botão deleta o relatório em questão da fila de geração de relatórios.

Relatórios gerados

A opção “**Relatórios gerados**” permite que o usuário visualize, realize o download do relatório desejado nos formatos “**PDF, TXT e HTML**”, ou delete um relatório permanentemente do sistema do Aker Report Center.

- O período de permanência dos relatórios gerados é definido na configuração de [ROTATE](#).



Visualização de relatórios

Aker Firewall

Eventos por Tipo de Log

Número de requisições por IP de destino

- 03/06/2015 15:12:17 x
- 03/06/2015 14:33:46 x
- 03/06/2015 14:10:14 x
- 03/06/2015 12:31:40 x
- 03/06/2015 11:48:52 x
- 03/06/2015 11:09:29 x
- 03/06/2015 10:44:51 x
- 03/06/2015 09:56:29 x
- 03/06/2015 09:18:51 x
- 03/06/2015 08:53:59 x
- 02/06/2015 18:23:07 x
- 02/06/2015 17:50:07 x
- 02/06/2015 16:33:45 x

Relatórios FTP

Requisições por IP de origem e destino

Data inicial: 02/06/2015 10:32 Data final: 03/06/2015 10:32

IP de origem: 10.4.69.4 IP de destino: 173.194.119.24

10 registros

IP origem	IP destino	Data/Hora
Não há registros para sua pesquisa		

1 a 1 de 1

PDF TXT HTML

Expandir

© 2015 - Aker Security Solutions - Todos os direitos reservados.

Figura 68 - Relatórios gerados

4.3 Agendamento

Na janela “**Agendamento**” o usuário pode visualizar os relatórios que já foram gerados no sistema, e configurar o agendamento automático de relatórios.

Agendamento de relatório

+ Agendar

10 registros

Buscar:

Nome do relatório	Data de início	
Requisições por IP de origem e destino	03/06/2015	☒ Editar ☒ Excluir
Detalhado	03/06/2015	☒ Editar ☒ Excluir

1 a 2 de 2

Figura 69 - Agendamento de relatório



Janela de agendamento de relatórios:

Agendamento de relatórios

Definir agendamento	Selecionar relatório
Repetir Diariamente Intervalo de repetição 1 Data de início 03/06/2015 Horário de execução 16:15 Finaliza ☒ Nunca ☐ Número de ocorrências ☐ Em data específica Diariamente, sem data de término	Relatório Requisições por IP de origem e destino Início da pesquisa Último dia
Parâmetros de pesquisa IP de origem IP de destino Entidade Todas Ativo Todos	
Opções de envio Enviar para teste@aker.com.br	
Salvar Voltar	

Figura 70 - janela de agendamento de relatórios

Cadastro





5 Cadastro

Este capítulo aborda as opções de cadastramento para: entidades, ativos, colunas, tipos de ativos, e relatórios no Aker Report Center.

O menu “**Cadastro**” permite que o usuário cadastre novas entidades, ativos, colunas, tipos de ativos, relatórios e grupos de relatórios que serão usados pelo Aker Report Center.

A seguir mais detalhes sobre as opções disponíveis para o menu *Cadastro*:

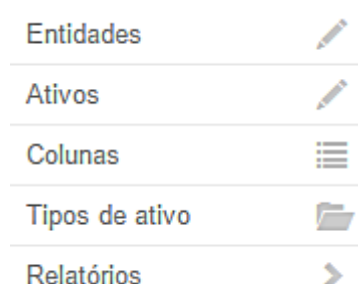


Figura 71 - menu cadastro

5.1 Entidades

Entidades são representações de um conjunto de informações sobre um determinado sistema, departamento, empresa, e etc. Por exemplo, uma entidade com o nome “**Empresa Matriz**”, a qual os **ativos** da empresa serão atribuídos (**computadores de usuários, servidores, impressoras e etc.**). Posteriormente estes **ativos** serão atribuídos aos usuários, de acordo com as permissões de acesso de cada usuário, dentro do sistema do Aker Report Center.

Nesta janela o usuário pode criar uma nova entidade, excluir e visualizar todas as entidades existentes no sistema.

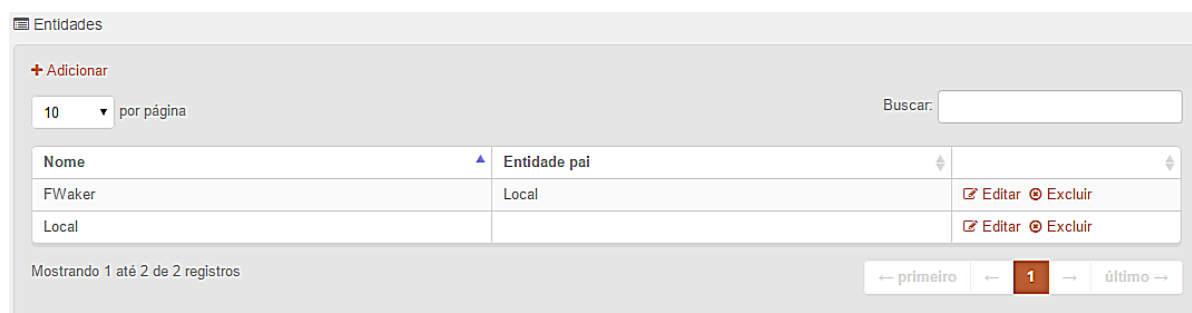
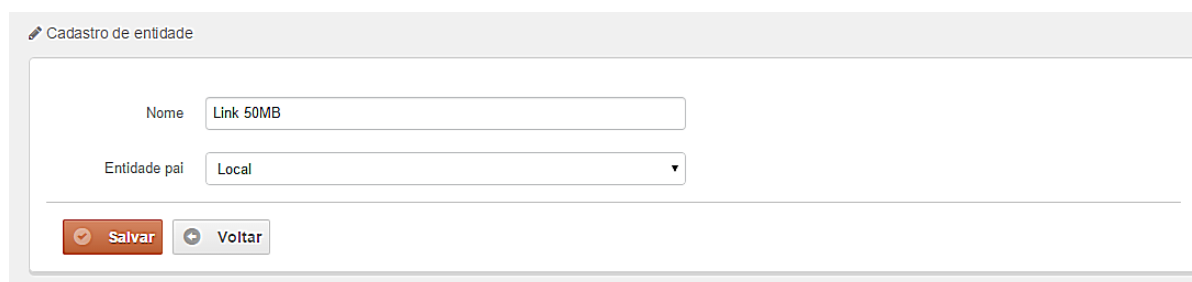


Figura 72 - Entidades

Janela de cadastramento de Entidade



Cadastro de entidade

Nome: Link 50MB

Entidade pai: Local

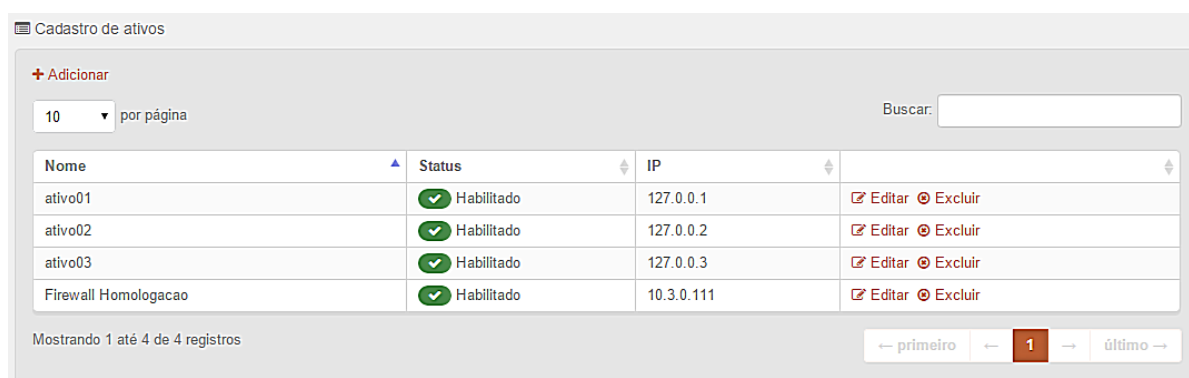
Salvar Voltar

Figura 73 - Cadastro de entidades

5.2 Ativos

Ativos são a representação de equipamentos/dispositivos de uma rede específica que possuem a capacidade de processamento de dados, ou seja, equipamentos/dispositivos que podem efetuar escolhas a partir de regras pré-definidas, como: **Roteadores, Switches, Computadores, Servidores e etc.**

Por meio desta janela o usuário pode criar, editar ou deletar “Ativos” do sistema do Aker Report Center.



+ Adicionar

10 por página

Buscar:

Nome	Status	IP	
ativo01	✓ Habilitado	127.0.0.1	Editar Excluir
ativo02	✓ Habilitado	127.0.0.2	Editar Excluir
ativo03	✓ Habilitado	127.0.0.3	Editar Excluir
Firewall Homologacao	✓ Habilitado	10.3.0.111	Editar Excluir

Mostrando 1 até 4 de 4 registros

← primeiro ← 1 → último →

Figura 74 - Cadastro de ativos

Cadastro de Ativos

Esta janela permite que o usuário visualize os ativos cadastrados no sistema, edite, delete ou adicione novos ativos. A seguir mais detalhes sobre como inserir um novo ativo no sistema do **Aker Report Center**:

Cadastro de ativos

[+ Adicionar](#)

10 por página

Buscar:

Nome	Status	IP	
ativo01	Habilitado	127.0.0.1	Editar Excluir
ativo02	Habilitado	127.0.0.2	Editar Excluir
ativo03	Habilitado	127.0.0.3	Editar Excluir
Firewall Homologacao	Habilitado	10.3.0.111	Editar Excluir

Mostrando 1 até 4 de 4 registros

← primeiro ← 1 → último →

Figura 75 - Cadastro de ativos

Cadastrando um novo Ativo

Para cadastrar um novo ativo siga os passos a seguir:

- Clique em [+ Adicionar](#) para que a janela de cadastro a seguir seja exibida:

Cadastro de ativo

[Cadastro de ativo](#) [Eventos Processados](#) [Eventos Não Processados](#)

Entidade

Nome

Interpretar arquivos recebidos? ☒ Sim ☐ Não

Salvar logs não interpretados? ☒ Sim ☐ Não

Tipo de ativo

Forma de envio de log ☒ Syslog ☐ FTP

Protocolo de envio ☒ UDP

IP

Hostname

Ativar fluxo ☒

[Salvar](#) [Voltar](#)

Figura 76 - Aba Cadastro de ativo



- Preencha os campos de aba “*Cadastro de ativo*” corretamente com a informação do ativo desejado, e clique em “*Salvar*”. A seguir mais detalhes sobre os campos da janela de cadastro de ativos:

Aba Cadastro de ativo

Nesta aba o usuário deve inserir as informações referentes ao ativo que será cadastrado:

Entidade: Neste campo o usuário deve selecionar a entidade que o novo ativo irá pertencer (para mais informações sobre Entidade veja o tópico “[Entidades](#)”)

Nome: Neste campo deve ser inserido o nome do novo “Ativo” que será cadastrado.

Interpretar arquivos recebidos: Ao selecionar “Sim” os relatórios prontos do Aker Firewall poderão ser vistos na aba ‘Relatórios Externos’, que fica na página principal.



Ao selecionar “**Sim**” os logs e arquivos **gerados e enviados** por esse ativo, poderão ser acessados na aba de relatórios recebidos (Dashboard). Quando esta opção está ativa, o envio de logs será realizado somente via FTP.

Salvar logs não interpretados:

Salvar logs não interpretados: Neste campo deve-se definir se este ativo gravará ou não logs não interpretados, ou seja, logs os quais não foram reconhecidos pelo *Aker Report Center*.

Tipo de ativo: Neste campo deve-se selecionar qual o tipo do ativo que está sendo criado.

Forma de envio de log: Nesta opção o usuário deve selecionar qual será o método de envio de log. As opções disponíveis são **Syslog e FTP** (mais informações sobre como cadastrar usuários FTP e configuração Syslog a seguir)



O envio de logs via FTP é possível apenas para arquivos “.TXT”, ou seja, apenas logs no formato “TXT” serão interpretados. Para que logs em outros formatos não sejam ignorados, é necessário selecionar a opção “**interpretar arquivos recebidos**”, para que o formato dos logs não importe e os mesmos possam ser visualizados na aba de Relatórios Externos.

- Ao selecionar a opção de envio FTP é necessário informar o nome do usuário FTP e o **caminho do diretório FTP** (no caminho do diretório não pode conter caracteres especiais, caso haja o sistema irá retirá-los).



Envio FTP

Forma de envio de log ☐ Syslog ☒ FTP

Usuário FTP

Diretório FTP

IP

Hostname

Figura 77 - Configuração de envio via FTP

Usuário FTP: usuário FTP que será usado na autenticação;

Diretório FTP: diretório FTP que armazenará os logs. Esse campo não pode ter espaços ou barras.

IP: IP da máquina que enviará o log.

Hostname: *hostname* da máquina que enviará o log (somente para identificação).

Envio Syslog

Forma de envio de log ☒ Syslog ☐ FTP

Protocolo de envio ☒ UDP

IP

Hostname

Figura 78 - Envio Syslog

Protocolo de envio: protocolo que será usado no recebimento de logs. As opções disponíveis são: **TCP, UDP, TCP/TLS**.

IP: IP da máquina que enviará o log.

Hostname: *Hostname* da máquina que enviará o log (somente para identificação).

Ativar Fluxo: Esta opção permite que usuário defina se o fluxo para este ativo estará ativo ou não.



A quantidade de ativos é limitada pela licença do usuário.



Ao configurar um Ativo é necessário configurar o firewall ou ativo em questão para que ele envie os logs para o Aker Report Center, siga os passos a seguir para fazer este procedimento no Aker Firewall:

- No firewall desejado acesse o menu “Configurações do sistema” e escolha a opção parâmetros de configuração;

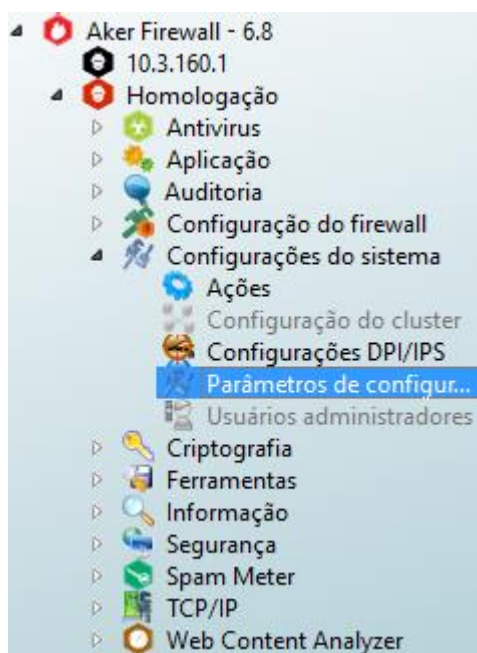


Figura 79 - Parâmetros de configuração

- Acesse a aba “Log”

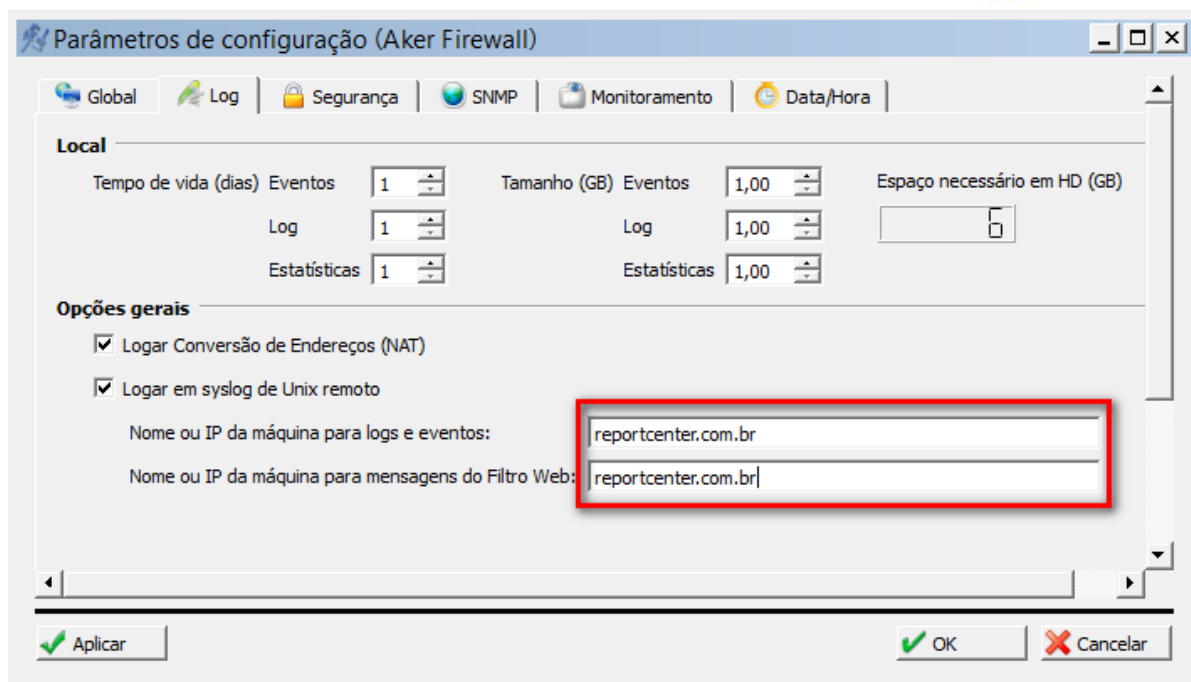


Figura 80 - Aba log

- Habilite a opção “Logar Conversão de Endereços (*NAT é opcional*)” e “Logar em syslog de Unix remoto”;
- Insira o nome da máquina ou IP que receberá os logs, eventos e mensagens do Filtro Web, no exemplo acima foi usado “reportcenter.br”.
- Clique em “OK” para confirmar a operação;
- É possível adicionar mais de uma máquina para o envio de logs e eventos. Para isso coloque o caractere ponto e vírgula (;) entre as máquinas, como exibido no exemplo abaixo:

AkerReportCenterfilial.com.br;AkerReportCentermatriz.com.br

10.3.70.202;10.3.70.204;10.4.29.2

Aba Eventos Processados

Esta aba exibe o número total de eventos que foram gerados pelo ativo em questão e os logs dos últimos eventos processados atualizando as informações a cada 5 segundos.



Cadastro de ativo	Eventos Processados	Eventos Não Processados
Total de eventos 336.028		
Últimos eventos		
<pre>dst_ip: www.aker.com.br, dst_port: 80, event_type: event, src_ip: 177.69.177.57, date: 2013-11-18 15:22:33, plugin_sid: 200, username: -, userdata1: GET / HTTP/1.0, userdata2: 10543, userdata3: http://letras.mus.br/ana-carolina/258918/, userdata4: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.0; Trident/5.0), filename: -, priority: notice, facility: user dst_ip: www.aker.com.br, dst_port: 80, event_type: event, src_ip: 177.69.177.57, date: 2013-11-18 15:22:33, plugin_sid: 200, username: -, userdata1: GET / HTTP/1.0, userdata2: 10545, userdata3: http://letras.mus.br/ana-carolina/258918/, userdata4: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.0; Trident/5.0), filename: -, priority: notice, facility: user dst_ip: www.aker.com.br, dst_port: 80, event_type: event, src_ip: 177.69.177.57, date: 2013-11-18 15:22:32, plugin_sid: 200, username: -, userdata1: GET / HTTP/1.0, userdata2: 10536, userdata3: http://letras.mus.br/ana-carolina/258918/, userdata4: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.0; Trident/5.0), filename: -, priority: notice, facility: user</pre>		

Figura 81 - Aba Eventos processados

Aba Eventos Não Processados

Esta aba exibe o número total de eventos que foram gerados e os logs dos últimos eventos processados pelo ativo em questão, mas ainda não foram processados.

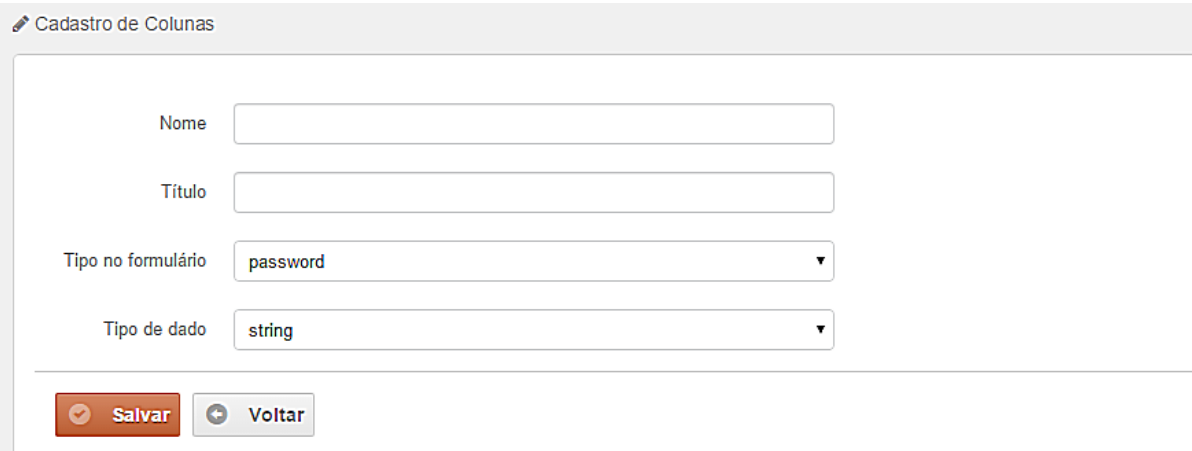
Cadastro de ativo	Eventos Processados	Eventos Não Processados
Total de eventos 4		
Últimos eventos		
<pre>Nov 18 15:23:33 www.aker.com.br: 80 177.69.177.57 - - [18/Nov/2013:15:23:33 -0200] "GET / HTTP/1.0" 200 10536 "http://ego.globo.com/famosos/noticia/2013/11/babi-rossi-sobre-affairs-de-olin-fez-cena- para-eu-ver-papel-de-crianca.html" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.57 Safari/537.36" Nov 18 15:23:33 www.aker.com.br: 80 177.69.177.57 - - [18/Nov/2013:15:23:33 -0200] "GET / HTTP/1.0" 200 10547 "http://letras.mus.br/luan-santana/ce-topa/" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.57 Safari/537.36" Nov 18 15:23:33 www.aker.com.br: 80 177.69.177.57 - - [18/Nov/2013:15:23:32 -0200] "GET / HTTP/1.0" 200 10539 "http://letras.mus.br/ana-carolina/258918/" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.0; Trident/5.0)" Nov 18 15:23:33 www.aker.com.br: 80 177.69.177.57 - - [18/Nov/2013:15:23:32 -0200] "GET / HTTP/1.0" 200 10540 "http://letras.mus.br/ana-carolina/258918/" "Mozilla/5.0 (compatible; MSIE 9.0; Windows</pre>		

Figura 82 - Aba Eventos não processados



5.3 Colunas

Por meio desta janela o usuário pode criar colunas personalizadas, as quais poderão ser utilizadas na geração de novos relatórios.

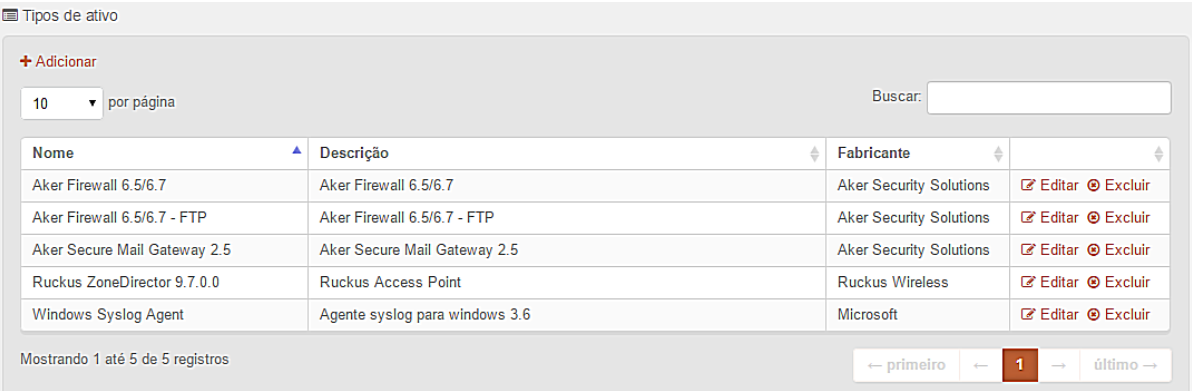


The image shows a web form titled "Cadastro de Colunas". It contains four input fields: "Nome" (text), "Título" (text), "Tipo no formulário" (dropdown menu with "password" selected), and "Tipo de dado" (dropdown menu with "string" selected). At the bottom, there are two buttons: "Salvar" (orange) and "Voltar" (grey).

Figura 83 - cadastro de colunas

5.4 Tipos de ativo

Na janela “**Tipos de ativo**” é possível que o usuário visualize, edite, exclua ou adicione um novo tipo de ativo no sistema do Aker Report Center. Atualmente, o Aker Report Center fornece 370 tipos de ativos para seus usuários.



The image shows a web interface titled "Tipos de ativo". It includes a "+ Adicionar" button, a pagination control showing "10 por página", and a search bar labeled "Buscar:". Below is a table with 5 columns: "Nome", "Descrição", "Fabricante", and two empty columns. The table contains 5 rows of data. At the bottom, there is a status bar "Mostrando 1 até 5 de 5 registros" and a pagination control with buttons for "primeiro", "1", and "último".

Nome	Descrição	Fabricante		
Aker Firewall 6.5/6.7	Aker Firewall 6.5/6.7	Aker Security Solutions	Editar	Excluir
Aker Firewall 6.5/6.7 - FTP	Aker Firewall 6.5/6.7 - FTP	Aker Security Solutions	Editar	Excluir
Aker Secure Mail Gateway 2.5	Aker Secure Mail Gateway 2.5	Aker Security Solutions	Editar	Excluir
Ruckus ZoneDirector 9.7.0.0	Ruckus Access Point	Ruckus Wireless	Editar	Excluir
Windows Syslog Agent	Agente syslog para windows 3.6	Microsoft	Editar	Excluir

Figura 84 - Tipos de ativos

A seguir detalhes sobre como adicionar um novo tipo de ativo.



5.4.1 Adicionando um novo tipo de ativo:

Para adicionar um novo tipo de ativo siga os passos descritos a seguir:

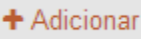
- Clique em  para que a janela de cadastro seja exibida:



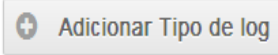
Figura 85 - Adicionando um novo tipo de ativo

- Preencha os campos de janela de cadastro de tipo de ativo corretamente:

Nome: nome do novo tipo de ativo (*ex: Aker Firewall 6.7*);

Descrição: descrição para o novo tipo de ativos (*ex: logs Aker Firewall 6.7*);

Fabricantes: nome do fabricante (*ex: Aker Security Solutions*);

Ao preencher os campos acima corretamente clique no botão , para configurar os tipos de log que serão registrados para o **tipo de ativo** em criação.



Adicionar Tipo de log

Nome Evento padrão

Expressão regular

```
(?:((?:\d{1,3}\.){3}\d{1,3})|(?:\w|\d|\.|\.|:|_|-|~|!|@|&|'|\"/>
```

Campo Selecione...

Inserir

Campos da expressão regular

Campo	Valor	
Campo de usuário 1	{ \$action }	✕ Excluir
Protocolo	{ \$protocol }	✕ Excluir
IP de destino	{ \$src_ip }	✕ Excluir
Porta de origem	{ \$src_port }	✕ Excluir

Cancelar

Adicionar

Figura 86 - Adicionando um novo tipo de log

Nome: o nome do tipo de log que será cadastrado (ex: *Evento padrão*).

Expressão regular: expressão regular para o tipo de ativo em criação, como no exemplo abaixo:

```
Aker_Firewall\:(?P<action>[ACDR])\s(?P<protocol>\w+)\s(?P<src_ip>(?:\d{1,3}\.){3}\d{1,3})|(?:\w|\d|\.|\.|:|_|-|~|!|@|&|'|\"/>
```

Campo: selecione os campos que serão usados no armazenamento dos logs.



Campo

Selecione...

Selecione...

Ação

Campo de usuário 2

Campo de usuário 3

Campo de usuário 4

Campo de usuário 5

Campo de usuário 6

Campo de usuário 7

Campo de usuário 8

Campo de usuário 9

Categoria

Comando

Data

Domínio

Download

dport

dst

Endereço IP

Endereço MAC

Flag

Inserir

Figura 87 - Seleção de campos

Ao selecionar o campo, é necessário que o usuário clique em ***“Inserir”*** para que o campo abaixo seja exibido.

Campos da expressão regular

Campo	Valor
Campo de usuário 1	{ \$action} ✖ Excluir
Protocolo	{ \$protocol} ✖ Excluir
IP de destino	{ \$src_ip} ✖ Excluir
Porta de origem	{ \$src_port} ✖ Excluir

Figura 88 - Campo de expressões regulares

Na listagem de expressões regulares acima, é necessário que o campo ***“Valor”*** seja preenchido corretamente para que o match seja efetuado, *ou seja, o processo que validará as informações, por exemplo, o campo “PROTOCOLO refere-se à { \$protocol} na expressão).*

- Clique em

Adicionar

, para concluir o cadastro.

5.5 Relatório

Por meio desta janela o usuário pode criar relatórios personalizados. A seguir mais informações sobre estas opções:

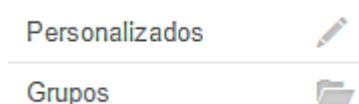


Figura 89 - Menu relatório

5.6 Relatórios personalizados

Nesta página o usuário pode criar, editar, excluir, e visualizar todos os modelos de relatórios personalizados no sistema do Aker Report Center.

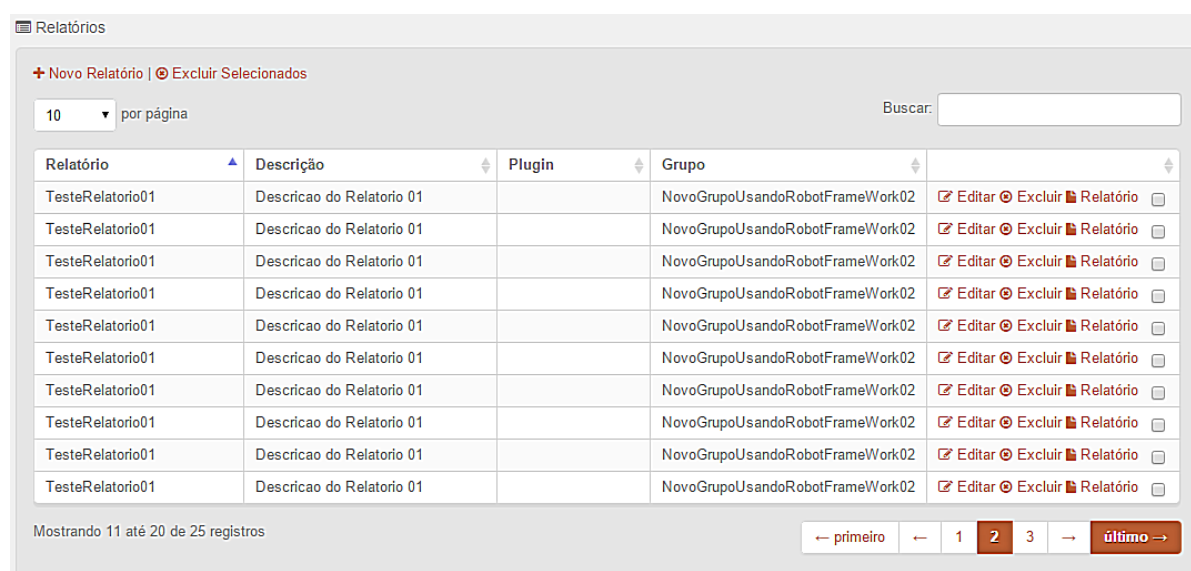
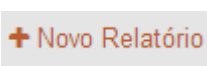


Figura 90 - relatório

Criando um novo de relatório do tipo detalhado.

Para criar um novo tipo de relatório siga os passos a seguir:

- Clique em , e preencha os campos das abas abaixo corretamente:



Aba Relatório

Nesta aba o usuário deve definir as informações básicas do novo relatório como: qual será o grupo, nome e tipo do relatório.

Figura 91 - Aba Relatório

Grupo: grupo que o relatório pertencerá. Para *mais informações veja tópico* [Grupos de relatórios](#).

Nome do relatório: nome que representará o relatório em criação.

Tipo: tipo do relatório. As opções disponíveis são: Detalhado ou consolidado.

Descrição: descrição sobre o relatório em criação.

Ao preencher os dados acima corretamente, clique em **Próximo**.

Aba Fonte de dados

Nesta aba o usuário deve selecionar qual o ativo ou tipos de ativos que serão carregados no relatório.



Relatório
Dados básicos

Fonte de dados
Ativos/Tipo de Ativo

Colunas
Colunas e Filtros

Parâmetros
Filtrar e salvar

Ativos

Selecionar os ativos ou um tipo de ativo para carregar no relatório

Ativo

Ativos
Firewall Homologação
Firewall de Borda
FW Homologação
FW Avalanche
FW cluster 2.35
TESTE de exclusão
Fw lab vpn
Firewall de Borda

Ativos Selecionados

Apache - Site Aker

Figura 92 - Aba Fonte de dados

Ao selecionar os ativos desejados, clique em **Próximo**.

Aba Colunas

Nesta aba o usuário deve selecionar as informações que serão exibidas ou não nas colunas do relatório.



Relatório

Dados básicos

Fonte de dados

Ativos/Tipo de Ativo

Colunas

Colunas e Filtros

Parâmetros

Filtrar e salvar

Configurar colunas

Coluna	Filtrar	Exibir	Obrigatório	Tamanho
Data	☐	☐	☐	00,00 %
IP de origem	☐	☐	☒	00,00 %
Porta de destino	☐	☐	☐	00,00 %
IP de destino	☐	☐	☐	00,00 %
Campo de usuário 1	☐	☐	☐	00,00 %
Campo de usuário 2	☐	☐	☐	00,00 %
Campo de usuário 3	☐	☐	☐	00,00 %
Nome de usuário	☐	☐	☐	00,00 %
Porta de origem	☐	☐	☐	00,00 %
Protocolo	☐	☐	☐	00,00 %
Interface	☐	☐	☐	00,00 %
times	☐	☐	☐	00,00 %
Comando	☐	☐	☐	00,00 %
URL	☐	☐	☐	00,00 %
Categoria	☐	☐	☐	00,00 %
Ação	☐	☐	☐	00,00 %
Mensagem	☐	☐	☐	00,00 %
Regra	☐	☐	☐	00,00 %
Perfil	☐	☐	☐	00,00 %
Upload	☐	☐	☐	00,00 %
Download	☐	☐	☐	00,00 %
Site	☒	☒	☐	00,00 %

Voltar

Salvar

« Anterior

Próximo »

Figura 93 - Aba Colunas

Filtrar: informações que serão filtradas no relatório, ou seja, filtros que serão exibidos no formulário de pesquisa do relatório em criação.

Exibir: informações que serão exibidas no relatório.

Tamanho: porcentagem que determinada informação irá ocupar no relatório.



A ordem das colunas pode ser alterada utilizando a função “*drag and drop*”.

Aba Parâmetros

Nesta aba o usuário deve selecionar quais os parâmetros que serão filtrados para exibir no relatório em criação.



Relatório Dados básicos	Parâmetros de filtro
Fonte de dados Ativos/Tipo de Ativo	
Colunas Colunas e Filtros	
Parâmetros Filtrar e salvar	

Parâmetro de pesquisa ▼

Operador... ▼

Valor do parâmetro

Adicionar

Parâmetro	
Nenhum filtro inserido	

Figura 94 - Aba Parâmetros de filtro

Parâmetro de pesquisa: Neste campo o usuário pode selecionar um parâmetro específico para exibição no relatório.

Parâmetro de pesquisa ▼

Parâmetro de pesquisa
Data
IP de origem
Campo de usuário 1
Campo de usuário 2
Campo de usuário 3
Campo de usuário 4
Nome de usuário
Tipo de Log

Figura 95 - Opções de parâmetros de pesquisa

Operador: Neste campo o usuário deve selecionar o “operador” que será usado na filtragem. Seguem as opções disponíveis:

Operador... ▼

Operador...
igual
diferente
maior
maior ou igual
menor
menor ou igual
em
não em
parecido

Figura 96 - Operador

Clique no botão “Adicionar” para concluir a inserção do parâmetro.

Ao preencher e configurar as abas acima corretamente, clique em “Salvar”.

Criando um novo de relatório do tipo Consolidado.

Para criar um novo tipo de relatório siga os passos a seguir:



- Clique em **+ Novo Relatório**, e preencha os campos das abas abaixo corretamente:

Aba Relatório

Nesta aba o usuário deve definir as informações básicas do novo relatório como: qual será o grupo, nome e tipo do relatório.

The screenshot shows the 'Dados básicos do relatório' (Basic report data) form. On the left is a sidebar with navigation options: 'Relatório Dados básicos' (selected), 'Fonte de dados Ativos/Tipo de Ativo', 'Colunas Colunas e Filtros', and 'Parâmetros Filtrar e salvar'. The main form area contains the following fields:

- Grupo:** A dropdown menu with 'Aker Firewall' selected.
- Nome do relatório:** A text input field containing 'Downloads'.
- Tipo:** A dropdown menu with 'Consolidado' selected.
- Ilimitado:** A checkbox that is checked.
- Descrição:** A text area containing 'Relatório de downloads Consolidado'.

At the bottom of the form are two buttons: 'Voltar' (grey) and 'Salvar' (orange). To the right of these are navigation buttons: '« Anterior' and 'Próximo »'.

Figura 97 - Aba Relatório

Grupo: grupo que o relatório pertencerá. Para *mais informações* veja tópico [Grupos de relatórios](#).

Nome do relatório: nome que representará o relatório em criação.

Tipo: tipo do relatório. As opções disponíveis são: Detalhado ou consolidado.

Ilimitado: Ao selecionar esta opção o relatório não terá um limite para a quantidade de linha.

Limite: Neste campo o usuário pode limitar a quantidade de linhas para seu relatório, por exemplo, 100 linhas.

Descrição: descrição sobre o relatório em criação.

Ao preencher os dados acima corretamente, clique em **Próximo**.

Aba Fonte de dados



Nesta aba o usuário deve selecionar qual o ativo ou tipos de ativos que serão carregados no relatório.

Relatório
Dados básicos

Fonte de dados
Ativos/Tipo de Ativo

Colunas
Colunas e Filtros

Parâmetros
Filtrar e salvar

Ativos

Selecionar os ativos ou um tipo de ativo para carregar no relatório

Ativo

Ativos	Ativos Selecionados
fw_borda	fw_homologacao
asmg	ftp_fw_homologacao
Secure	-0

Voltar Salvar « Anterior Próximo »

Figura 98 - Aba Fonte de dados

Ao selecionar os ativos desejados, clique em

Próximo

Aba Colunas

Nesta aba o usuário deve selecionar as informações que serão exibidas ou não nas colunas do relatório.

Relatório
Dados básicos

Fonte de dados
Ativos/Tipo de Ativo

Colunas
Colunas e Filtros

Parâmetros
Filtrar e salvar

Configurar colunas

Coluna	Filtrar	Exibir	Obrigatório	Tamanho
sensor	☐	☒	☐	00,00 %
Data	☐	☐	☐	00,00 %
IP de origem	☐	☐	☐	00,00 %
Porta de destino	☐	☐	☐	00,00 %
IP de destino	☐	☐	☐	00,00 %
Campo de usuário 1	☐	☐	☐	00,00 %
Campo de usuário 2	☐	☐	☐	00,00 %
Campo de usuário 3	☐	☐	☐	00,00 %
Campo de usuário 4	☐	☐	☐	00,00 %
Campo de usuário 5	☐	☐	☐	00,00 %
Campo de usuário 6	☐	☐	☐	00,00 %
Campo de usuário 7	☐	☐	☐	00,00 %

Figura 99 - Aba Colunas



Filtrar: informações que serão filtradas no relatório, ou seja, filtros que serão exibidos no formulário de pesquisa do relatório em criação.

Tamanho: porcentagem que determinada informação irá ocupar no relatório.

Agrupar: ao selecionar está opção a coluna em questão terá suas informações agrupadas para a coluna em questão.

Operação de agrupamento: neste campo deve-se definir o tipo de agrupamento que será realizada na coluna definida abaixo. As opções disponíveis são: Somatório e contagem de registro.

Coluna a realizar operação: neste campo deve-se selecionar a coluna que receberá a operação de agrupamento definida acima.



A ordem das colunas pode ser alterada utilizando a função “*drag and drop*”.

Aba Parâmetros

Nesta aba o usuário deve selecionar quais os parâmetros que serão filtrados para exibir no relatório em criação.

Figura 100 - Aba Parâmetros de filtro

Parâmetro de pesquisa: Neste campo o usuário pode selecionar um parâmetro específico para exibição no relatório.

Figura 101 - Opções de parâmetros de pesquisa

Operador: Neste campo o usuário deve selecionar o “operador” que será usado na filtragem. Seguem as opções disponíveis:

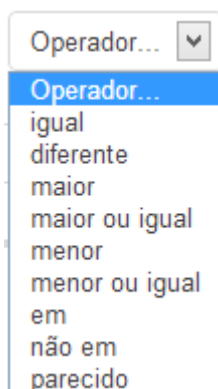


Figura 102 - Operador

Clique no botão “Adicionar” para concluir a inserção do parâmetro.

Ao preencher e configurar as abas acima corretamente, clique em “Salvar”.

5.7 Grupos de relatórios

Esta opção permite que o usuário visualize, crie ou delete grupos de relatórios.

Grupos de relatórios

+ Novo Grupo de Relatório

10 por página

Buscar:

Grupo	
10	☒ Editar ☒ Excluir
11	☒ Editar ☒ Excluir
11	☒ Editar ☒ Excluir
12	☒ Editar ☒ Excluir
12	☒ Editar ☒ Excluir
13	☒ Editar ☒ Excluir
13	☒ Editar ☒ Excluir
14	☒ Editar ☒ Excluir
14	☒ Editar ☒ Excluir
15	☒ Editar ☒ Excluir

Mostrando 1 até 10 de 51 registros

← primeiro ← 1 2 3 4 5 → último →

Nome: Ativos Aker

☒ Salvar ☒ Voltar

Figura 103 – Janela de criação de Grupo de relatórios

Configurações



6 Configurações

Este capítulo mostra como configurar as variáveis do sistema do Aker Report Center.

O menu “**Configurações**” permite que o usuário defina as configurações de autenticação, rede, backup, rotate, e-mail, serviços, exportação de logs, e a visualização das ações executados no sistema do Aker Report Center.

Autenticação	>
Rede	>
Backup	>
Rotate	C
E-mail	✉
Serviços	⚙
Exportação	>
Logs do sistema	☰

Figura 104 - menu configurações

6.1 Autenticação

Por meio deste menu é possível configurar de forma rápida e fácil todos os aspectos de autenticação do Aker Report Center, como: *Perfis, Usuários, Tipos de autenticação e FTP TLS*.

Perfis	👤
Usuários	👤
Usuários FTP	👤
Tipo de autenticação	🔒
FTP TLS	⚙

Figura 105 – Autenticação



Perfis

Na janela “**Perfis**” é possível visualizar todos os perfis usuários existentes no sistema, além de editar, excluir e adicionar um novo perfil de usuário no sistema.



Figura 106 - Perfil

Janela de cadastro de perfil

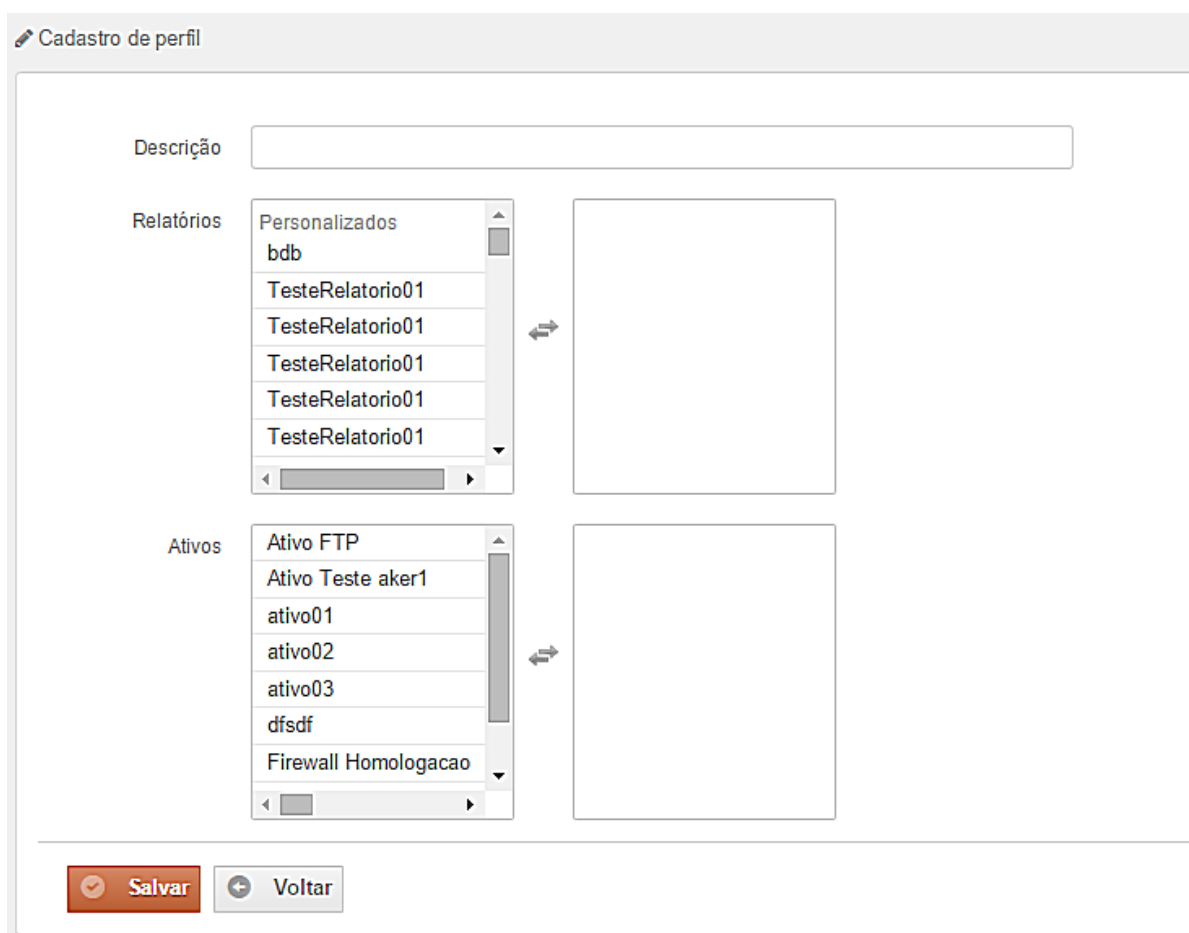


Figura 107 - Janela Perfil



Usuários

Na janela “**Usuários**” é possível visualizar todos os perfis de usuários existentes no sistema do Aker Report Center, além de editar, excluir, e adicionar um novo usuário no sistema.

Nome	Ações
Edilson Moura	Editar Excluir
edilson2	Editar Excluir
Fernando Araújo Bagno da Silva	Editar Excluir
Lucas Pereira	Editar Excluir
lucas-admin	Editar Excluir
teste	Editar Excluir

Figura 108 - Usuários

Usuários FTP

Por meio da janela “**Usuários FTP**” o administrador pode visualizar os usuários FTP existentes no sistema, editar, deletar ou adicionar novos usuários FTP.

Nome	Ações
aker	Editar Excluir
lucas	Editar Excluir

Figura 109 - Usuários FTP

Para cadastrar um novo usuário FTP siga os passos abaixo:

- Na janela de usuários FTP clique em **+ Adicionar**:



Cadastro de usuário FTP

Usuário	Paulo
Password	

Figura 110 - Cadastro de usuário FTP

- Insira o nome do novo usuário e sua respectiva senha, e então clique em  para finalizar o cadastro do novo usuário FTP.

Tipo de autenticação

Na aba “**Tipo de autenticação**” o usuário deve selecionar qual o tipo de autenticação que será efetuada:

- **Não:** Ao selecionar “**Não**”, a autenticação será efetuada por meio de uma base local (banco de dados do sistema).
- **Sim:** Ao selecionar “**Sim**”, a autenticação será efetuada por meio de uma base LDAP.

Autenticação

Utilizar autenticação via LDAP?	Sim
Host	10.10.10.10
Base DN	DC=network,DC=USer,DC=com,DC=br
Domínio	mydomain.user.com.br

Figura 111 - Autenticação



FTP TLS

Por meio da janela “**FTP TLS**” o usuário pode definir se a conexão segura será usada ou não para os usuários que se conectarem via FTP. Caso escolha “**Sim**” para usar conexão segura no FTP, o usuário deverá definir se a conexão TLS será obrigatória ou não.

Selecionando “**Sim**”, para obrigar conexão TLS, fará com que apenas conexões TLS sejam permitidas. Selecionando “**Não**” conexões **TLS e FTP** serão permitidas. Nesta janela também é possível carregar a chave e o certificado do servidor que serão usados para criptografar a conexão.

Configurações de segurança FTP

Usar conexão segura no FTP (TLS) Este campo é obrigatório.

Obrigar conexão TLS

Chave

Certificado

Informações do certificado

```
-----BEGIN CERTIFICATE-----
MIIDKjCCApOgAwIBAgIJAN5NhqFgDv7WMA0GCSqGSIb3DQE
BBQUAMIGtMQswCQYD
VQQGEwJCUjERMA8GA1UECAwIQnJhc2lzaWExCzAJBgNVBAc
MAkRGMSAwHgYDVQK
DBdBa2VyIFN1Y3VyaXR5IFNvbHV0aW9uczEYMBYGA1UECww
PRGVzZW52b2x2aW1l
bnRvMRgwFgYDVQDDA93d3cuYWt1ci5jb20uYnIxKDAmBgk
qhkiG9w0BCEW9z
ZW1hcy52aWVpcmFAYWt1ci5jb20uYnIwHhcNMTMwODI2MTc
```

Figura 112 - Configuração de segurança FTP

6.2 Rede

Este submenu permite que o usuário defina as configurações do servidor NTP e interface de rede do Aker Report Center.



Interfaces de rede



Servidores NTP



Figura 113 - rede

Interface de rede

Na janela “**Interfaces de rede**” o usuário pode configurar as interfaces de rede da máquina que o Aker Report Center está instalado.

Figura 114 - Interface de rede

Interface: Neste campo o usuário deve selecionar a interface de rede que será configurada para o Aker Report Center;

Método: O Aker Report Center oferece dois métodos de configuração de redes para seus usuários, que são:

- **DHCP** – para utilizar este método o usuário deve ter um servidor DHCP na rede para pegar o IP manualmente.



- **Estático** – ao selecionar este método o usuário deve configurar a rede manualmente preenchendo os dados a seguir:

IP: Neste campo o usuário deve definir o IP do Aker Report Center;

Rede: Neste campo o usuário deve definir o IP da rede do usuário;

Broadcast: Neste campo o usuário deve definir o IP de broadcast;

Máscara de rede: Neste campo o usuário deve definir máscara de rede em uso;

Gateway: Neste campo o usuário deve inserir o gateway da rede;

Servidor DNS: Neste campo o usuário pode inserir o servidor de DNS da rede do usuário. Para inserir um DNS secundário insira uma vírgula (,) entre **os endereços DNS**

Exemplo: 10.0.0.150,10.0.0.200

Servidores NTP

Na janela “**Servidores NTP – Network Time Protocol**” o usuário configura os servidores NTP que serão usados para sincronizar a hora do servidor mantendo-a sempre exata.



Apenas os servidores da <http://www.pool.ntp.org/en/> serão aceitos.

⊙ Servidores NTP

Servidor 1	
Servidor 2	
Servidor 3	
Servidor 4	

Figura 115 - Servidores NTP

6.3 Backup

O submenu “**Backup**” permite que o usuário crie backups de suas configurações ou carregue um backup o qual foi previamente salvo. Este submenu possui duas opções que serão abordadas a seguir:



Realizar backup



Restaurar backup



Figura 116 - Opções de backup

Realizar backup

A opção “**Realizar backup**” permite que o usuário salve um backup das configurações do Aker Report Center.

Para fazer o backup das configurações do Aker Report Center, navegue até o menu “**Configurações**”, clique no submenu “**Backup**”, abra a janela “**Realizar backup**” e clique em

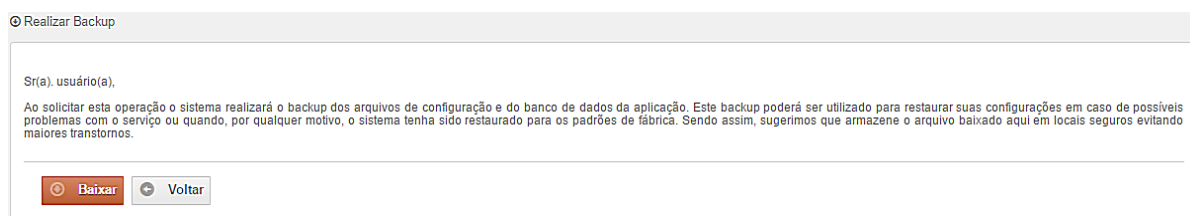


Figura 117 -Janela Realizar Backup

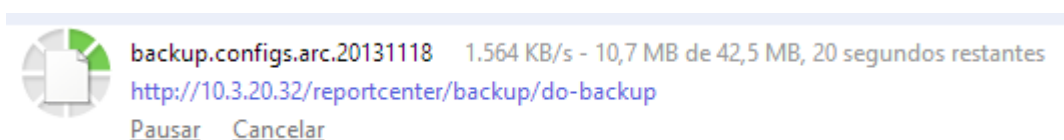


Figura 118 - Criação de backup

Restaurar backup

A janela “**Restaurar backup**” permite que o usuário restaure as configurações do Aker Report Center através da utilização de um backup previamente salvo.



Este procedimento excluirá toda e qualquer informação contida nas configurações em uso, salvando apenas as configurações contidas no backup.

Para restaurar um backup siga os passos a seguir:



- Clique no botão  .
- Localize o arquivo que será usado para restaurar as configurações do *Aker Report Center* e clique em “**Abrir**”;

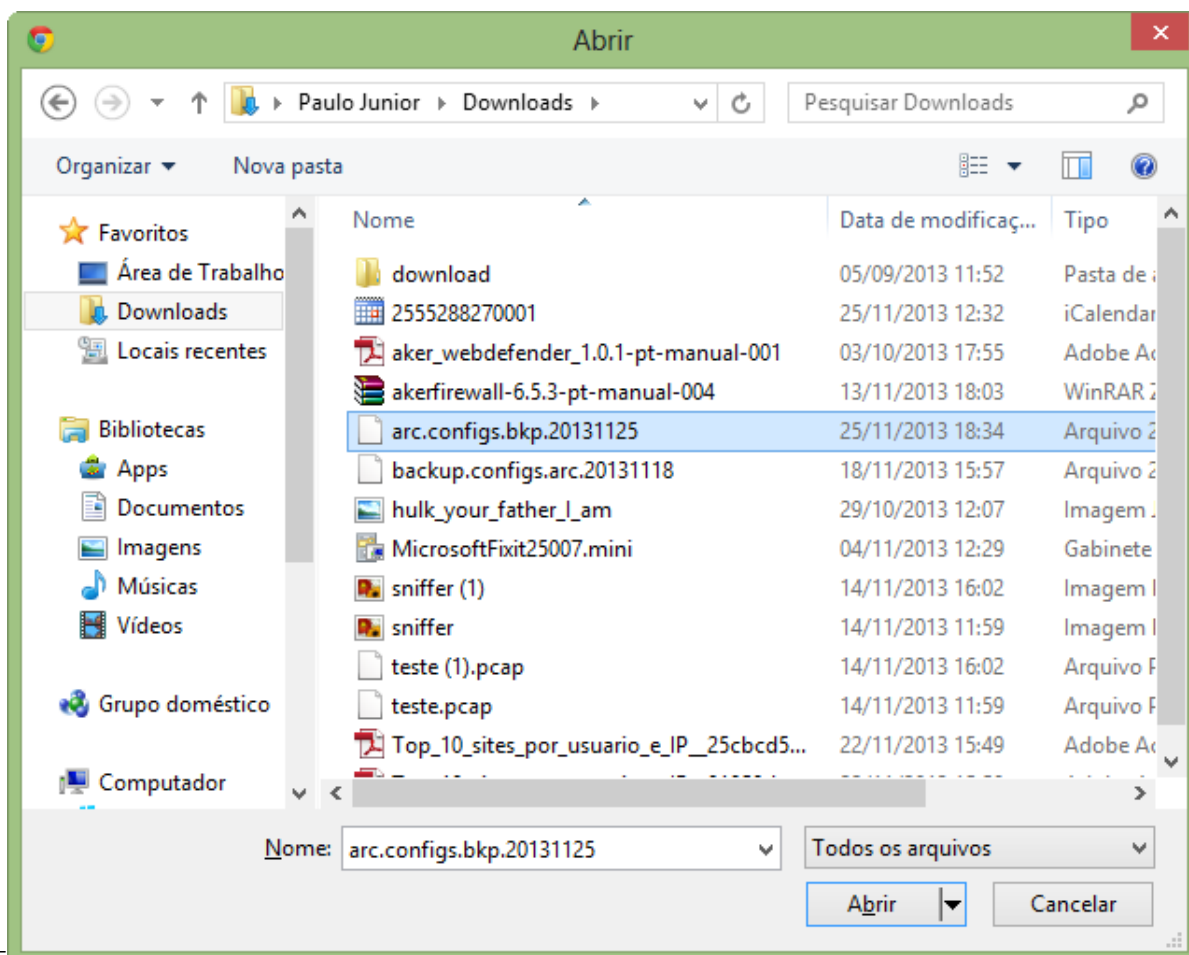


Figura 119 - localizando arquivo de backup

- Clique em  .

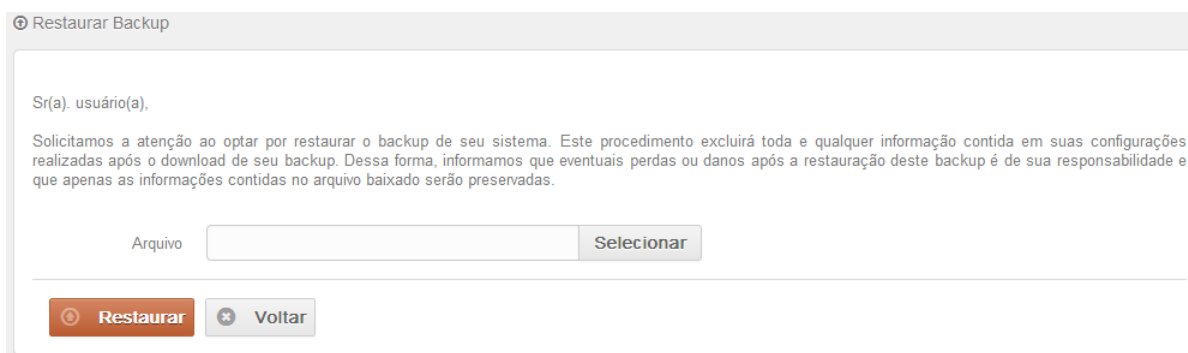
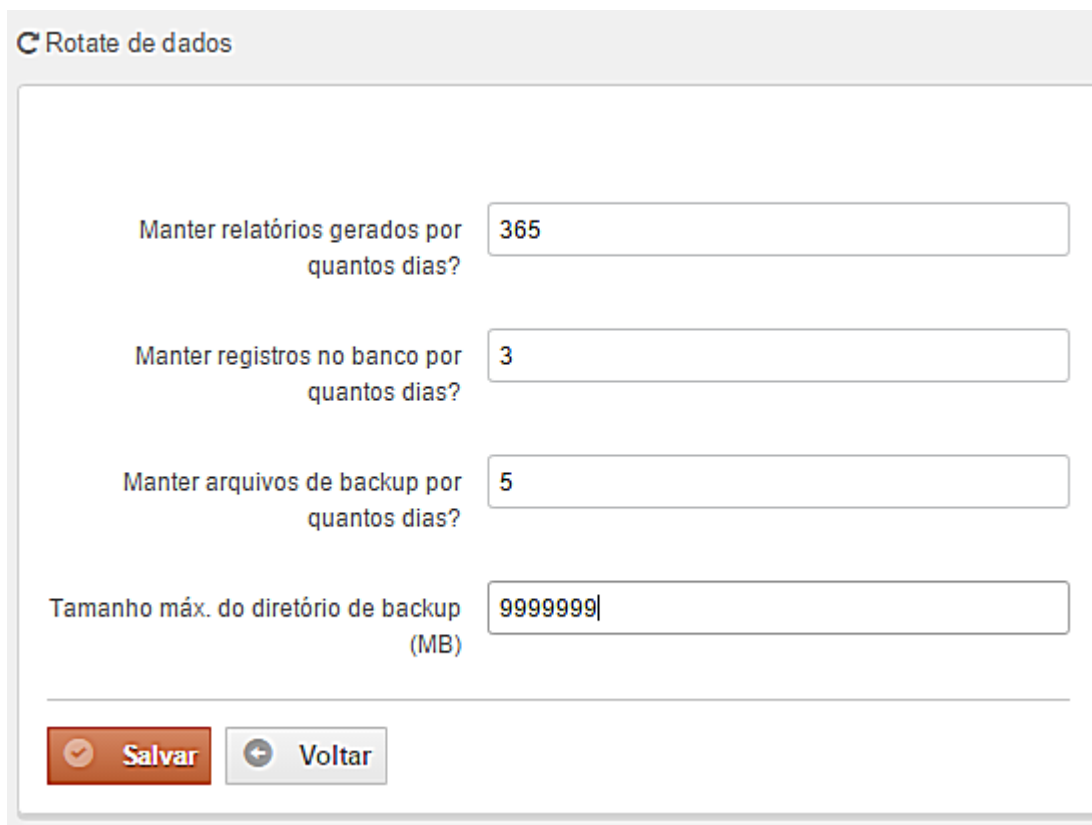


Figura 120 - Janela Restaurar Backup



6.4 Rotate

Na janela “**Rotate**” o usuário pode definir as configurações de armazenamento dos logs e relatórios gerados, a quantidade de dias que os registros serão mantidos no servidor, se os registros excluídos serão salvos em um diretório ou não, por quanto tempo os backups serão mantidos e o tamanho máximo do diretório que armazenará os backups.



Rotate de dados

Manter relatórios gerados por quantos dias? 365

Manter registros no banco por quantos dias? 3

Manter arquivos de backup por quantos dias? 5

Tamanho máx. do diretório de backup (MB) 9999999

Salvar Voltar

Figura 121 - Rotate

Manter Relatórios gerados por quantos dias: Neste campo o usuário deve definir a quantidade de dias que os relatórios gerados serão mantidos no banco de dados;

Manter registros no banco por quantos dias: Neste campo o usuário deve definir a quantidade de dias que os registros (logs) serão mantidos no banco de dados;

Manter backup por quantos dias: Neste campo o usuário deve definir a quantidades de dias que o backup de registros excluídos será mantido no sistema;

Tamanho máx. do diretório de backup (MB): Neste campo o usuário deve definir o tamanho máximo que será usado do diretório de backup para armazenar os registros excluídos.



Todos os logs recebidos pelo Aker Report Center serão enviados para o diretório de backup automaticamente. Caso o limite de armazenamento de backup seja atingido, os arquivos de backup antigos serão removidos, para que os novos sejam armazenados.



6.5 E-mail

A janela “**E-mail**” permite que o usuário configure o e-mail que será usado para enviar os relatórios gerados pelo Aker Report Center, além de definir uma conta de e-mail que sempre receberá notificações do Aker Report Center, em situações como por exemplo, quando a licença do usuário estiver prestes a expirar. A seguir detalhes sobre os campos da janela “**E-mail**”.

□ Configurações de E-mail

Servidor ReportCenter	https://100.1.1.0
Servidor smtp	smtp.live.com
Porta	25
Autenticação	Nenhum
Método de Autenticação	Nenhum
Usuário	user@live.com.br
Senha	
Enviar e-mails de	reportcenter@live.com.br
Enviar e-mails para	user@live.com.br; admin@live.com.br

Figura 122 - Configuração de E-mail

Servidor Report Center: Neste campo deve-se inserir o endereço do servidor do Aker Report Center.



Servidor de e-mail: Neste campo deve-se inserir o endereço do servidor de e-mail que será utilizado para enviar os e-mails do Aker Report Center.

Porta: Neste campo deve-se inserir o número da porta que será usada para enviar os e-mails do Aker Report Center

Autenticação: Neste campo define-se a autenticação do usuário será solicitada ou não para baixar o e-mail no servidor.

Método de autenticação: Neste campo deve-se selecionar qual o método de autenticação usado para que o usuário possa fazer o download do e-mail no servidor.

Usuário: Neste campo deve-se inserir o nome de usuário da conta que enviará as notificações do Aker Report Center.

Senha: Neste campo deve-se inserir a senha do usuário da conta que enviará as notificações do Aker Report Center.

Enviar e-mails de: Neste campo deve-se inserir o e-mail que será usado para enviar s e-mails do Aker Report Center.

Enviar e-mails para: Neste campo deve-se inserir os e-mails que receberam notificações do Aker Report Center.

6.6 *Serviços*

Este menu permite que o usuário configure a quantidade de analisadores (parsers) que estarão funcionando simultaneamente, e as configurações do banco de dados.

Mais detalhes sobre estes campos a seguir:



Configurações de Serviços

Parser

Número de serviços

Banco de dados (Logs)

Servidor

Usuário

Senha

Banco de dados (Configuração)

Servidor

Nome da base

Usuário

Senha

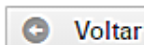
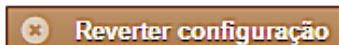
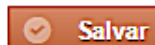


Figura 123 - Janela de configuração de serviços

Parser

- **Número de serviços:** Neste campo o usuário deve selecionar a quantidade de analisadores (parsers) que estarão rodando simultaneamente (*é recomendado que este número seja o mesmo da quantidade de processadores da máquina, exemplo, “número de serviços 5, número de processadores 4”*).

Banco de dados (logs)

- **Servidor:** Neste campo o usuário deve inserir o endereço do servidor de banco de dados (logs)
- **Usuário:** Neste campo deve-se inserir o nome de usuário para acessar o servidor de banco de dados (este campo pode ser deixado em branco);
- **Senha:** Neste campo deve-se a senha de acesso para a autenticação no servidor de banco de dados (este campo pode ser deixado em branco);

Banco de dados (configuração)



- **Servidor:** Neste campo o usuário deve-se inserir o endereço do servidor de banco de dados (configuração);
- **Nome da base:** Neste campo deve-se inserir o nome do banco de dados de configuração o padrão é Aker Report Center;
- **Usuário:** Neste campo deve-se inserir o nome de usuário para acessar o servidor de banco de dados;
- **Senha:** Neste campo deve-se inserir a senha de acesso para a autenticação no servidor de banco de dados;

6.7 Exportação

Este menu permite que o usuário configure o envio de dados de um *Aker Report Center* para outro *Aker Report Center*, por exemplo, o *Aker Report Center* de uma ou várias *filiais* enviando seus dados para uma *Matriz*, possibilitando o gerenciamento centralizado dos ativos como exibido no exemplo abaixo:

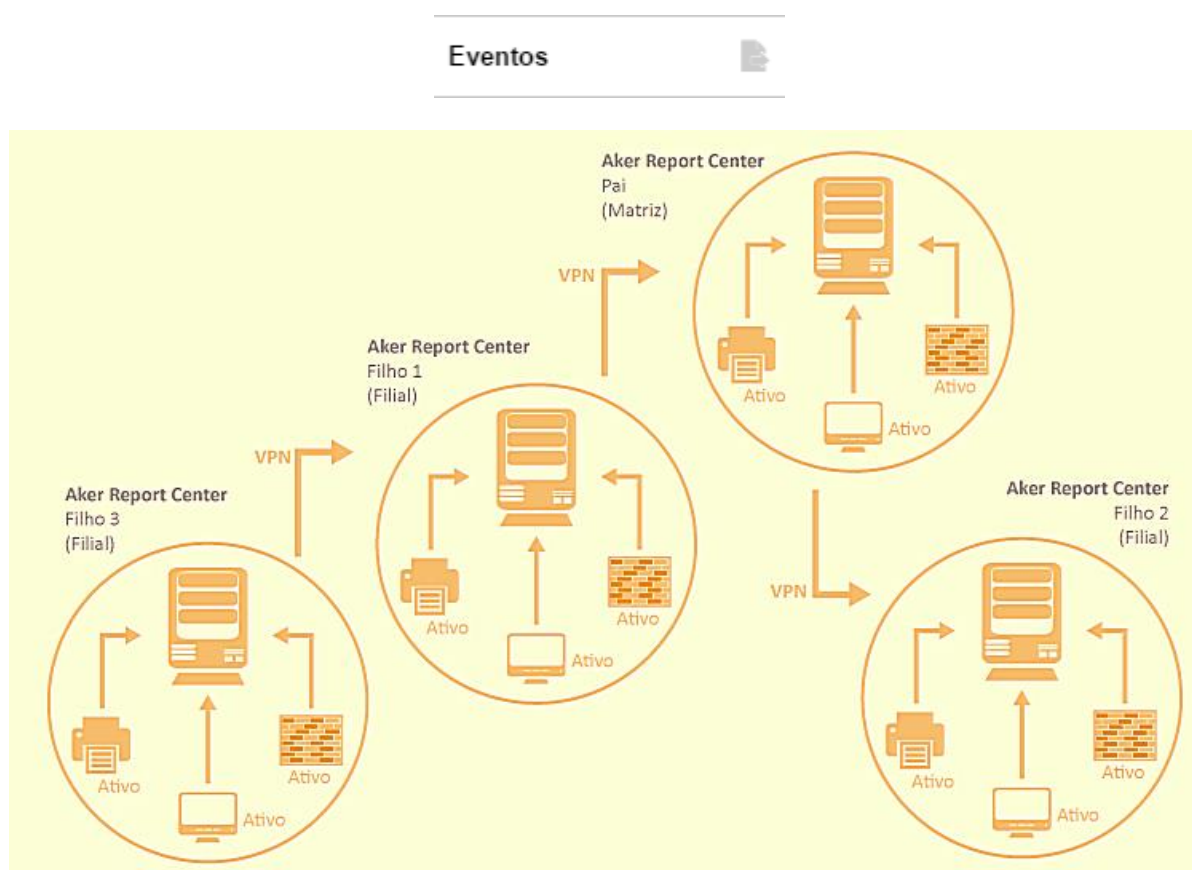


Figura 124 - Esquema de exportação de dados



Neste exemplo os Aker Report Centers filhos 1, 2, e 3 estão enviando os dados (logs, eventos, etc.) de seus ativos via FTP para o Aker Report Center da Matriz, possibilitando um gerenciamento de dados centralizado na matriz.

A seguir detalhes da janela de agendamento de exportação de dados:

Figura 125 - Janela de exportação de eventos

Servidor FTP: Neste campo o usuário deve inserir o caminho do servidor que irá receber os dados;

Diretório remoto: Neste campo o usuário deve inserir o diretório remoto usado na conexão FTP. Este diretório deve ser o mesmo especificado na criação do ativo ([Menu Cadastro – Ativos – Cadastro de Ativos](#)).

6.8 Logs do sistema

Por meio desta janela o usuário pode visualizar as ações que foram executadas no sistema do Aker Report Center.

Logs do sistema

10 por página

Data	Tipo	Mensagem
30/06/2015 10:40:09	Info	Relatório Eventos por Tipo de Log gerado
30/06/2015 10:40:09	Info	Relatório Eventos por Tipo de Log gerado
30/06/2015 10:35:49	Info	Relatório ReportCountLogtype enviado para fila.
30/06/2015 10:35:35	Warning	Ocorreu um erro 404 - Página não encontrada.
30/06/2015 10:35:35	Warning	Ocorreu um erro 404 - Página não encontrada.
30/06/2015 10:35:32	Info	O usuário admin se autenticou no sistema.
30/06/2015 10:34:42	Info	O usuário admin se autenticou no sistema.
30/06/2015 10:34:31	Info	Relatório Eventos por Tipo de Log gerado
30/06/2015 10:34:31	Info	Relatório Eventos por Tipo de Log gerado

Mostrando 1 até 10 de 129,200 registros

← primeiro 1 2 3 4 5 → último →

Figura 126 - Logs do sistema

6.9 Ajuda

Por meio desta janela o usuário tem acesso ao manual do Aker Report Center, fórum da Aker, e ações referentes à: licenciamento e atualizações.

Licenciamento	>
Atualizações	↺
Fórum Aker	🔗
Manual	⬇

6.10 Licenciamento

Esta janela permite que o usuário configure os parâmetros de sua licença. Ao concluir a instalação do sistema do Aker Report Center, no primeiro login o usuário deve gerar a chave de licenciamento do produto.



Ao gerar a chave de licenciamento o usuário deve enviar a mesma, juntamente com o nome o qual a chave foi licenciada para licenca@aker.com.br solicitando sua licença.



Gerar Chave

Ao concluir a instalação do sistema Aker Report Center, o usuário deve acessar o endereço designado para o Aker Report Center em seu navegador, e utilizar o nome de usuário e senha exibidos a seguir para efetuar o login no sistema **(a interface de rede é configurada por padrão em modo DHCP)**.

- Senha padrão Interface texto

Usuário padrão SSH: aker

Senha padrão SSH: 123456

- Senha padrão Interface remota

Usuário padrão: admin

Senha padrão: 123456



O número máximo de tentativas para logar-se no **Aker Report Center** são 3, caso o usuário exceda este número máximo de tentativas, terá que esperar 2 minutos para tentar efetuar o login novamente.

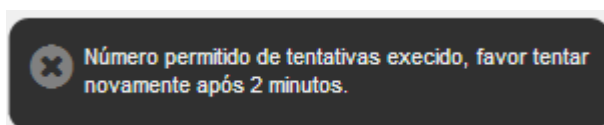


Figura 127 - Mensagem ao errar a senha mais de 3 vezes

The login screen for Aker Report Center features the company logo at the top left. Below it, the text 'Aker Report Center' is displayed. The login form consists of two input fields: 'Login' with the text 'admin' and 'Senha' with masked characters '.....'. An orange 'Entrar' button is positioned below the password field. At the bottom of the form, there is an information icon and the text 'Favor entrar com seu login e senha.'

Figura 128 - Tela de login



No primeiro login o usuário deve gerar a chave de licenciamento do produto. Ao gerar a chave de licenciamento o usuário deve enviar esta chave para licenca@aker.com.br solicitando sua licença.

Para gerar a chave de licenciamento do produto e carregar a licença do produto siga os passos abaixo:

- Preencha o campo “Licenciado para” e clique em .

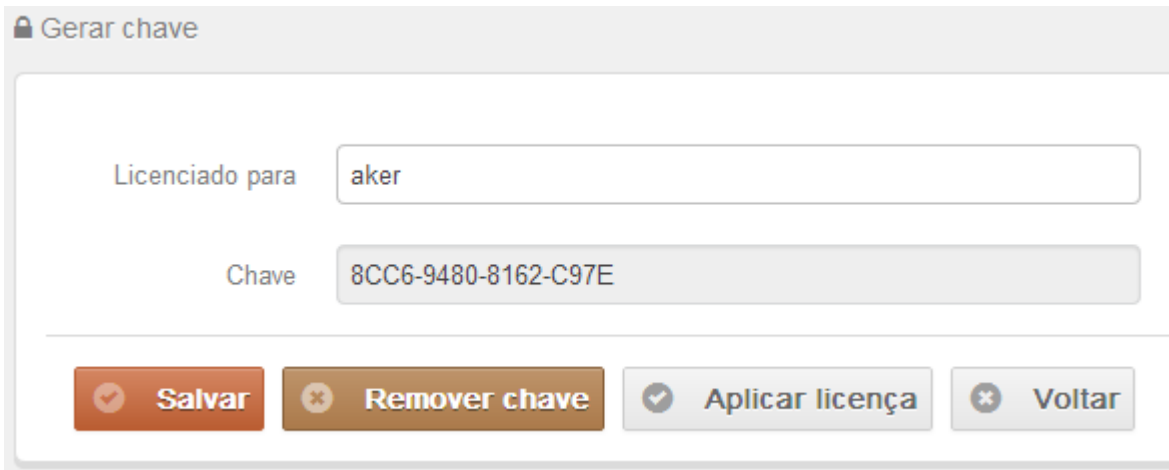
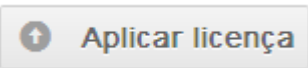


Figura 129 - Gerar chave

Licenciando para: Neste campo deve-se informar o nome do usuário ou empresa para qual o produto está sendo licenciado.

Chave: Ao preencher o campo “Licenciado para” e clicar em “**Salvar**” fará com que uma chave de licenciamento seja gerada automaticamente. O usuário deve encaminhar esta chave para licenca@aker.com.br solicitando sua licença. Ao receber a licença siga os passos a seguir *(ao enviar a solicitação o usuário receberá sua licença no período máximo de 24h).*

- Ao receber a licença clique em 
- Na janela Aplicar Licença clique no ícone  para localizar sua licença.

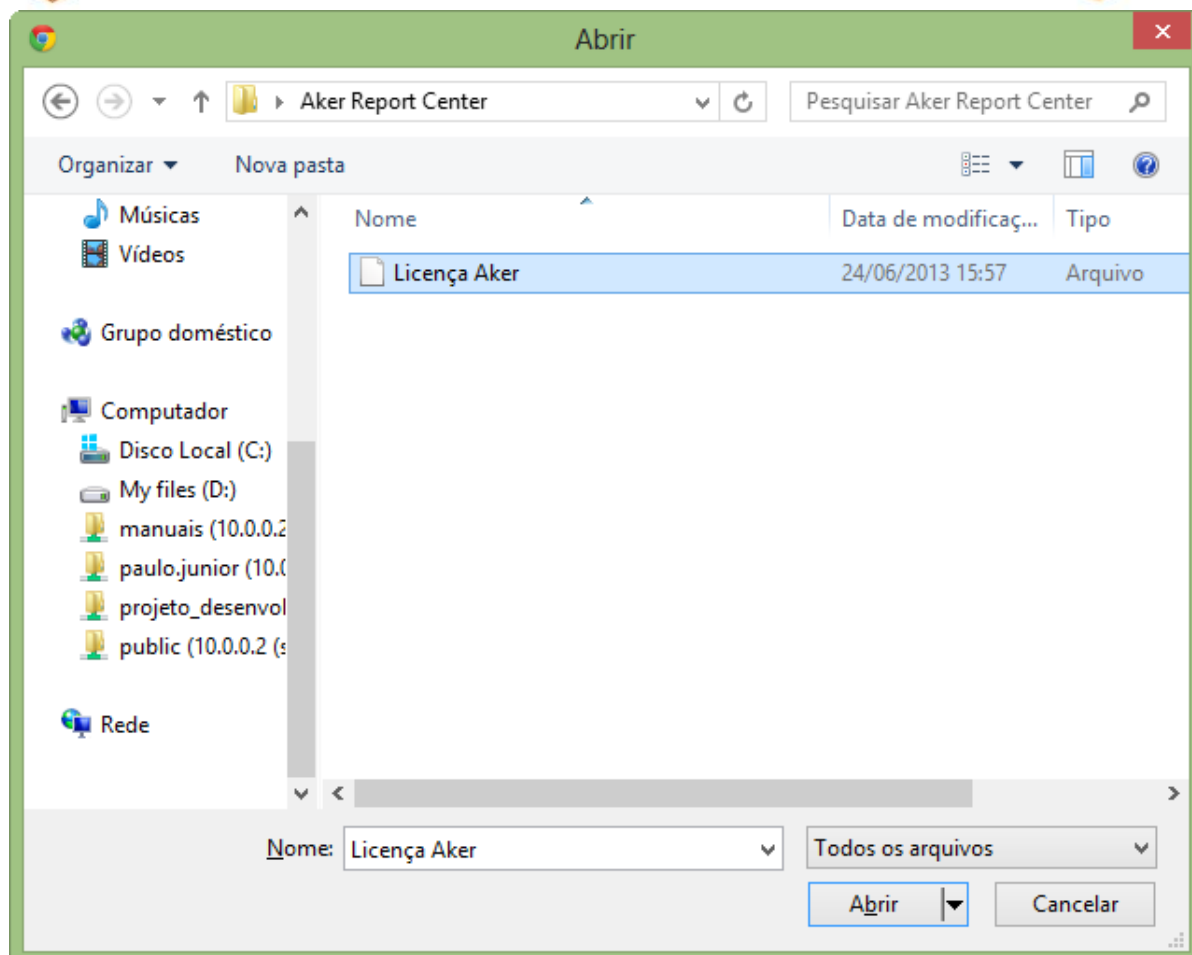


Figura 130 - Localizando licença



Figura 131 - Opções de carregamento da licença

- Ao localizar o arquivo clique no ícone  para carregar o arquivo. Ao carregar a licença suas informações serão exibidas na mesma tela como na imagem a seguir:



✓ Aplicar Licença

Informações da Licença

Nome	aker
Serial	200000020697
Data de expiração	30/01/2014
Nº de ativos	20
Quantidade de eventos	250.000.000

Figura 132 - Informação da licença

Após carregar a licença, serão exibidas as informações sobre sua licença:

Nome: Neste campo é exibido o nome do titular da licença;

Serial: Neste campo é exibido o serial da licença em uso/carregada;

Data de expiração: Neste campo é exibido a data de expiração da licença em uso/carregada;

Nº de ativos: Neste campo é exibido o número de ativos suportados pela licença em uso/carregada ativo para a licença em questão;

Quantidades de eventos: Neste campo é exibido a quantidade de eventos suportados pela licença em uso;



Esta janela permite que o usuário visualize as informações da licença em uso, lembrando que ao carregar uma nova licença as informações serão atualizadas, desta forma, somente as informações da licença em uso serão exibidas.

Depois de completar o processo de upload da licença no sistema, serão exibidas as informações da licença, clique no botão  depois do upload para completar processo de licenciamento.

Atualizações

Esta janela permite que o usuário configure o sistema do Aker Report Center para que as atualizações sejam carregadas automaticamente selecionando o período desejado. Ao carregar as atualizações, as mesmas serão exibidas na lista de atualizações disponíveis, para



que o usuário decida qual atualização ele deseja aplicar. Clique na opção “**Aplicar**” para atualizar o sistema.

Figura 133 - Atualizações

Baixar atualizações: Neste campo o usuário deve selecionar o período o qual o sistema do Aker Report Center irá baixar as atualizações e disponibiliza-las na lista de atualizações disponível. A seguir as opções de período disponíveis:

Figura 134 - Opções para baixar atualizações

Enviar atualizações baixadas manualmente: Esta opção permite que o usuário realize o upload de atualizações manualmente. A atualização será exibida na lista de “**Atualizações disponíveis**” para que a mesma seja aplicada.

Fórum Aker

Esta opção redirecionará o usuário para a página do “*Fórum da Aker*”, aonde o usuário pode tirar dúvidas, iniciar e participar de debates.

Manual

Ao clicar nesta opção o usuário será redirecionado para a página do manual do Aker Report Center.



6.11 *Opções de gerenciamento da conta do usuário*

Estas opções ficam localizadas no lado superior direito da tela, e por meio delas o usuário pode visualizar ou alterar suas informações de forma rápida ou sair do sistema do Aker Report Center.

